# TOTAL ACCESS 850
## System Manual

| | |
|---|---|
| **1200375L1** | **Total Access 850 Chassis** |
| **1200373L1** | **T1 Bank Controller Unit (BCU)** |
| **1200373L2** | **T1 BCU with DSX Port** |
| **4200376L1#TDM** | **T1 Router Control Unit (RCU) with TDM Software** |
| **4200376L1#ATM** | **T1 RCU with ATM Software** |
| **1200377L1** | **SDSL RCU** |
| **1203384L1** | **Echo Canceller** |
| **1203384L2** | **Echo Canceller with ADPCM** |
| **1175006L2** | **Power Supply Unit** |
| **1175043L2** | **AC Supply/Battery Charger** |

64200376L1-1A
April 2003

## Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, or trade names of their respective holders.

## To the Holder of the Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000

## About this Manual

This manual provides a complete description of the Total Access 850 system and system software. The purpose of this manual is to provide the technician, system administrator, and manager with general and specific information related to the planning, installation, operation, and maintenance of the Total Access 850. This manual is arranged so that needed information can be quickly and easily found. The following is an overview of the contents.

Provides instructions for configuring and using the ADTRAN Utilities software programs including Telnet, VT100, and TFTP.

Provides the MIB compilation order and the MIBs, Traps, and MIB Variables supported by the unit.

## Revision History

This is the first issue of this manual.

*In this manual, unit refers to the Total Access 604, 608, 612, 616, and 624. If a statement only applies to a particular unit, the unit will be specified by number.*

NOTE *Notes provide additional useful information.*

CAUTION *Cautions signify information that could prevent service interruption.*

WARNING *Warnings provide information that could prevent damage to the equipment or endangerment to human life.*

## Safety Instructions

When using your telephone equipment, please follow these basic safety precautions to reduce the risk of fire, electrical shock, or personal injury:

1. Do not use this product near water, such as a bathtub, wash bowl, kitchen sink, laundry tub, in a wet basement, or near a swimming pool.
2. Avoid using a telephone (other than a cordless-type) during an electrical storm. There is a remote risk of shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.
4. Use only the power cord, power supply, and/or batteries indicated in the manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for special disposal instructions.

## Save These Important Safety Instructions

FCC regulations require that the following information be provided in this manual:

1. This equipment complies with Part 68 of FCC rules. On the back of the equipment housing is a label showing the FCC registration number and ringer equivalence number (REN). If requested, provide this information to the telephone company.
2. If this equipment causes harm to the telephone network, the telephone company may temporarily discontinue service. If possible, advance notification is given; otherwise, notification is given as soon as possible. The telephone company will advise the customer of the right to file a complaint with the FCC.
3. The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of this equipment. Advance notification and the opportunity to maintain uninterrupted service are given.
4. If experiencing difficulty with this equipment, please contact ADTRAN for repair and warranty information. The telephone company may require this equipment to be disconnected from the network until the problem is corrected or it is certain the equipment is not malfunctioning.
5. This unit contains no user-serviceable parts.
6. An FCC compliant telephone cord with a modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using an FCC compatible modular jack, which is Part 68 compliant.
7. The following information may be required when applying to the local telephone company for leased line facilities.

| Network Port | Service Type | REN/SOC | FIC | USOC |
|---|---|---|---|---|
| T1/FT1/ISDN PRI | 1.544 Mbps - SF<br>1.544 Mbps - SF and B8ZS<br>1.544 Mbps - ESF<br>1.544 Mbps - ESF and B8ZS | 6.0N | 04DU9-BN<br>04DU9-DN<br>04DU9-1KN<br>04DU9-1SN | RJ-48C |
| FXO/FXS | Analog Loop Start | 2.9A | 02LS2 | RJ-21X |

8. The REN is useful in determining the quantity of devices you may connect to your telephone line and still have all of those devices ring when your number is called. In most areas, the sum of the RENs of all devices should not exceed five. To be certain of the number of devices you may connect to your line as determined by the REN, call your telephone company to determine the maximum REN for your calling area.
9. This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs. Contact your state public utility commission or corporation commission for information.

## Affidavit Requirements for Connection to Digital Services

- An affidavit is required to be given to the telephone company whenever digital terminal equipment without encoded analog content and billing protection is used to transmit digital signals containing encoded analog content which are intended for eventual conversion into voiceband analog signals and transmitted on the network.

- The affidavit shall affirm that either no encoded analog content or billing information is being transmitted or that the output of the device meets Part 68 encoded analog content or billing protection specifications.
- End user/customer will be responsible for filing an affidavit with the local exchange carrier when connecting unprotected customer premise equipment (CPE) to 1.544 Mbps or subrate digital services.

Until such time as subrate digital terminal equipment is registered for voice applications, the affidavit requirement for subrate services is waived.

## Affidavit for Connection of Customer Premises Equipment to 1.544 Mbps and/or Subrate Digital Services

**For the work to be performed in the certified territory of ___________________ (telco name)**

**State of ________________**

**County of ________________**

**I, ______________________ (name), ___________________________________ (business address),**

**____________________ (telephone number) being duly sworn, state:**

**I have responsibility for the operation and maintenance of the terminal equipment to be connected to 1.544 Mbps and/or ________ subrate digital services. The terminal equipment to be connected complies with Part 68 of the FCC rules except for the encoded analog content and billing protection specifications. With respect to encoded analog content and billing protection:**

( ) I attest that all operations associated with the establishment, maintenance, and adjustment of the digital CPE with respect to analog content and encoded billing protection information continuously complies with Part 68 of the FCC Rules and Regulations.

( ) The digital CPE does not transmit digital signals containing encoded analog content or billing information which is intended to be decoded within the telecommunications network.

( ) The encoded analog content and billing protection is factory set and is not under the control of the customer.

**I attest that the operator(s)/maintainer(s) of the digital CPE responsible for the establishment, maintenance, and adjustment of the encoded analog content and billing information has (have) been trained to perform these functions by successfully having completed one of the following (check appropriate blocks):**

( ) A. A training course provided by the manufacturer/grantee of the equipment used to encode analog signals; or

( ) B. A training course provided by the customer or authorized representative, using training materials and instructions provided by the manufacturer/grantee of the equipment used to encode analog signals; or

( ) C. An independent training course (e.g., trade school or technical institution) recognized by the manufacturer/grantee of the equipment used to encode analog signals; or

( ) D. In lieu of the preceding training requirements, the operator(s)/maintainer(s) is (are) under the control of a supervisor trained in accordance with _________ (circle one) above.

**I agree to provide ______________________ (telco's name) with proper documentation to demonstrate compliance with the information as provided in the preceding paragraph, if so requested.**

**__________________________________Signature**

**__________________________________Title**

**__________________________________ Date**

**Transcribed and sworn to before me**

**This ________ day of _______________, _______**

**__________________________________**
**Notary Public**

**My commission expires:**

**__________________________________**

## Federal Communications Commission Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio frequencies. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

NOTE *Shielded cables must be used with this unit to ensure compliance with Class A FCC limits.*

WARNING *Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.*

## Industry Canada Compliance Information

Notice: The Industry Canada label applied to the product (identified by the Industry Canada logo or the “IC:” in front of the certification/registration number) signifies that the Industry Canada technical specifications were met.

Notice: The Ringer Equivalence Number (REN) for this terminal equipment is supplied in the documentation or on the product labeling/markings. The REN assigned to each terminal device indicates the maximum number of terminals that can be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices should not exceed five (5).

## Canadian Emissions Requirements

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioelectriques applicables aux appareils numériques de Class A prescrites dans la norme sur le materiel brouilleur: “Appareils Numériques,” NMB-003 edictee par le ministre des Communications.

## Warranty and Customer Service

ADTRAN will repair and return this product within ten  years from the date of shipment if it does not meet its published specifications or fails while in service. For detailed warranty, repair, and return information refer to the ADTRAN Equipment Warranty and Repair and Return Policy Procedure.

Return Material Authorization (RMA) is required prior to returning equipment to ADTRAN.

For service, RMA requests, or further information, contact one of the numbers listed at the end of this section.

## LIMITED PRODUCT WARRANTY

ADTRAN warrants that for ten  years from the date of shipment to Customer, all products manufactured by ADTRAN will be free from defects in materials and workmanship. ADTRAN also warrants that products will conform to the applicable specifications and drawings for such products, as contained in the Product Manual or in ADTRAN's internal specifications and drawings for such products (which may or may not be reflected in the Product Manual). This warranty only applies if Customer gives ADTRAN written notice of defects during the warranty period. Upon such notice, ADTRAN will, at its option, either repair or replace the defective item. If ADTRAN is unable, in a reasonable time, to repair or replace any equipment to a condition as warranted, Customer is entitled to a full refund of the purchase price upon return of the equipment to ADTRAN. This warranty applies only to the original purchaser and is not transferable without ADTRAN's express written permission. This warranty becomes null and void if Customer modifies or alters the equipment in any way, other than as specifically authorized by ADTRAN.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE FOREGOING CONSTITUTES THE SOLE AND EXCLUSIVE REMEDY OF THE CUSTOMER AND THE EXCLUSIVE LIABILITY OF ADTRAN AND IS IN LIEU OF ANY AND ALL OTHER WARRANTIES (EXPRESSED OR IMPLIED). ADTRAN SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING (WITHOUT LIMITATION), ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.   SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THIS EXCLUSION MAY NOT APPLY TO CUSTOMER.

In no event will ADTRAN or its suppliers be liable to the Customer for any incidental, special, punitive, exemplary or consequential damages experienced by either the Customer or a third party (including, but not limited to, loss of data or information, loss of profits, or loss of use). ADTRAN is not liable for damages for any cause whatsoever (whether based in contract, tort, or otherwise) in excess of the amount paid for the item. Some states do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to the Customer.

## Customer Service, Product Support Information, and Training

ADTRAN will repair and return this product if within ten  years from the date of shipment the product does not meet its published specification or the product fails while in service.

A return material authorization (RMA) is required prior to returning equipment to ADTRAN. For service, RMA requests, training, or more information, use the contact information given below.

### Repair and Return

If you determine that a repair is needed, please contact our Customer and Product Service (CAPS) department to have an RMA number issued. CAPS should also be contacted to obtain information regarding equipment currently in house or possible fees associated with repair.

| | |
|---|---|
| CAPS Department | (256) 963-8722 |

Identify the RMA number clearly on the package (below address), and return to the following address:

ADTRAN Customer and Product Service<br>
901 Explorer Blvd. (East Tower)<br>
Huntsville, Alabama 35806

RMA # _____________

### Pre-Sales Inquiries and Applications Support

Your reseller should serve as the first point of contact for support. If additional pre-sales support is needed, the ADTRAN Support web site provides a variety of support services such as a searchable knowledge base, latest product documentation, application briefs, case studies, and a link to submit a question to an Applications Engineer. All of this, and more, is available at:

http://support.adtran.com

When needed, further pre-sales assistance is available by calling our Applications Engineering Department.

| | |
|---|---|
| Applications Engineering | (800) 615-1176 |

### Post-Sale Support

Your reseller should serve as the first point of contact for support. If additional support is needed, the ADTRAN Support web site provides a variety of support services such as a searchable knowledge base, updated firmware releases, latest product documentation, service request ticket generation and trouble-shooting tools. All of this, and more, is available at:

http://support.adtran.com

When needed, further post-sales assistance is available by calling our Technical Support Center. Please have your unit serial number available when you call.

| | |
|---|---|
| Technical Support | (888) 4ADTRAN |

### Installation and Maintenance Support

The ADTRAN Custom Extended Services (ACES) program offers multiple types and levels of installation and maintenance services which allow you to choose the kind of assistance you need. This support is available at:

http://www.adtran.com/aces

For questions, call the ACES Help Desk.

| | |
|---|---|
| ACES Help Desk | (888) 874-ACES (2237) |

### Training

The Enterprise Network (EN) Technical Training Department offers training on our most popular products. These courses include overviews on product features and functions while covering applications of ADTRAN's product lines. ADTRAN provides a variety of training options, including customized training and courses taught at our facilities or at your site. For more information about training, please contact your Territory Manager or the Enterprise Training Coordinator.

| | |
|---|---|
| Training Phone | (800) 615-1176, ext. 7500 |
| Training Fax | (256) 963-6700 |
| Training Email | training@adtran.com |

# SYSTEM DESCRIPTION

## CONTENTS

## 1. SYSTEM OVERVIEW

The Total Access 850 is an integrated access device designed for cost-effective deployment of voice and data services at the customer premises. The Total Access 850 system benefits integrated communications providers, such as CLECs, ILECs, and ISPs, who require a customer premises device that integrates voice and data functions, and provides a viable migration path from TDM to packet-based technology (see *Modules* on page 19 for details). The Total Access 850 features remote management, an integrated IP router, and special services slots.

The Total Access 850 is a modular device with two common slots, six access slots for FXS, FXO, Dual V.35, and UBR1TE modules, and two slots for special access modules. The FXS, FXO, Dual V.35, and UBR1TE modules are supported in the Router Control Unit (RCU); however, the Bank Controller Unit (BCU) also supports E&M and OCU DP modules. Using local or remote inband management, carriers can turn features, functions and access ports on and off. Easy access to modules, common modules, power supplies, and the battery back-up system simplifies maintenance procedures. Hot-swappable modules may be replaced without disrupting other units. The four-circuit-per-module design ensures that only four analog circuits are affected when replacing a module.

A compact, NEBS-compliant cabinet suitable for the customer premises or the central office provides added safety and reliability. The 2U design uses little rack space. When wall mounted, the 8½-inch by 11-inch chassis occupies a space the size of a piece of notebook paper. Two Total Access 850 systems can be mounted side-by-side in either 19-inch or 23-inch relay racks. Preconfigured packages are available.

## 2. FEATURES AND BENEFITS

Below is a list of Total Access 850 features and benefits. Some features are module-dependent.

### Configuration and Management

- VT100 Emulation
- SNMP Management (with RCU)
- Telnet (with RCU)
- Dial-up remote management via external analog modem
- Six levels of password protection and privileges (with RCU)

### Software Upgradeable

- Flash memory
- TFTP download (with RCU)
- XMODEM via control port

### Signaling Support

- T1/FT1 integrated access
- TDM to ATM migration (with RCU)
- Upgradeable to DSL using SDSL RCU
- TR-08 signaling support
- Analog FXS and FXO voice expansion (four per module)

### Integrated Components (with RCU)

- IP router
- DSX-1 T1/PBX interface
- V.35 Nx56/64 DTE interface

### Testing

- Local and remote: payload/line, V.54 (depending on installed modules)
- Patterns: 511, QRSS, all ones, all zeros (depending on installed modules)

### Performance Monitoring

- Reports: Information stored for last 24 hours in 15 minute increments
- Performance statistics per TR54016, T1.403, RFC1406
- Alarm reporting per TR54016, T1.403

## 3. MODULES

The Total Access 850 has six system modules, three system resource modules, and six access modules:

### *System Modules*

- Bank Controller Unit (BCU) (P/N 1200373L1)
- BCU with Fractional T1 (P/N 1200373L2)
- T1 Router Control Unit (RCU) with TDM software (P/N 4200376L1#TDM)
- T1 Router Control Unit (RCU) with ATM software (P/N 4200376L1#ATM)
- SDSL RCU (P/N 1200377L1)
- Power Supply Unit (P/N 1175006L2)

### *Resource Modules*

- Echo Canceller with ADPCM (P/N 1203384L2)
- Echo Canceller without ADPCM (P/N 1203384L1)
- Nx56/64K Data Service Unit (DSU) (P/N 1200372L1)

### *Access Modules*

- Quad FXS Access Module (P/N 1175408L2)
- Quad FXO Access Module (P/ N 1175407L2)
- OCU DP Access Module (P/N 1180005L1)
- UBR1TE Access Module (P/N 1180020L1)
- E&M/TO Access Module (P/N 1180402L1)
- Dual V.35 Access Module (P/N 1180025L1)
- DSX-1 Access Module (P/N 1200385L1)
- Single DS0 DP Access Module (P/N 1180003L1) - requires a BCU (L1 or L2) when installed in Total Access 850

Each access module is hot-swappable with configuration restored upon replacement.

NOTE *Replacing an access module with a different module type will result in configuration loss.*

### Total Access 850 Bank Controller Unit (BCU) (P/N 1200373L1)

In addition to controlling the shelf and its contents, the BCU serves as the user interface. The operator provisions and monitors all modules in the system either locally or remotely, via the BCU interface. The BCUs provision the option cards in the shelf via the faceplate DB-9 Admin connector of the active system controller and a VT100 terminal.

### BCU with Fractional T1 (P/N 1200373L2)

The BCU L2 is like the L1 version discussed above, but it also has a DSX/Fractional T1 interface.

### T1 Router Control Unit (RCU) (P/N 4200376L1#TDM and 4200376L1#ATM)

The RCU has an integrated router, FT1 port, and Nx56/64K port. The RCU can be provisioned locally via the DB-9 connector on the faceplate, or the RJ-45 craft connector on the back of the chassis. A 10BaseT Ethernet connector is provided on the back for access to the integrated IP router.

### SDSL RCU (P/N 1200377L1)

The SDSL RCU has an integrated router and an Nx56/64k DTE port. The SDSL RCU can be provisioned locally via the DB-9 connector located on the faceplate or the RJ-45 craft connector on the back of the chassis. Additionally, a 10BaseT Ethernet connector is provided on the back for access to the integrated IP router. The SDSL RCU supports 2B1Q SDSL on the network interface with rates from 160 kbps to 2.3 Mbps.

### Echo Canceller without ADPCM (P/N 1203384L1)
### Echo Canceller with ADPCM (P/N 1203384L2)

An Echo Canceller Module is available for use with the ATM version of the T1 RCU. Echo cancellation and ADPCM resources are built into the SDSL version of the RCU, so this module is not required when using the SDSL RCU. The Echo Canceller Module provides G.168 echo cancellation for voice over ATM applications and is available with or without Adaptive Differential Pulse Code Modulation (ADPCM). ADPCM is a speech coding method which uses fewer bits than traditional Pulse Code Modulation (PCM), allowing the user to get more analog voice calls on less bandwidth. These modules must be installed in system resource slots A and B.

NOTE *The Echo Canceller module ADPCM functionality automatically shifts ON/OFF when fax or modem calls are placed. To find out the current status of the Echo Canceller functionality, check the current status of each FXS port. The path of the current status can be found at the following path:* ***L2 PROTOCOL > STATUS > PVC STATUS > PROTOCOL STATUS > POTS STATS > CODING TYPE*** *(this will display either PCM of ADPCM).*

## Power Supply Unit (P/N 1175006L2)

The power supply unit (PSU) supplies -48 VDC and 20 Hz ringing voltage to the BCUs, RCUs, and access modules. The PSU converts -48 VDC input to the required voltages needed to operate all common units and access modules. The ring generator circuit provides 20 Hz ring voltage to the analog voice access modules.

## Nx56/64K Module (P/N 1200372L1)

This module is only used with the BCU L1 or L2 (1200373L1 or 1200373L2) to activate the V.35 port on the rear of the chassis. Insert this module into system resource slots A and B.

## Quad FXS Access Module (P/N 1175408L2)

The Quad FXS Module provides analog voice extension for the Total Access 850 platform. Four analog voice ports are used to connect to analog phones. The Quad FXS Module supports Foreign Exchange Subscriber, Dial Pulse Terminate (DPT), and Private Line Automatic Ringdown (PLAR) and provides Ground Start/Loop Start to E&M conversion capability.

## Quad FXO Access Module (P/N 1175407L2)

The Foreign Exchange Office (FXO) module interfaces to the Central Office switch and to an FXS or RPOTS card over a T1 facility. Four analog voice ports on the FXO access module provide four individual connections to the switch. The FXO supports standard Loop Start and Ground Start options as well as Dial Pulse Terminate (DPT) functionality. Up to six Quad FXO Access Modules may be installed in the Total Access 850.

## OCU DP Access Module (P/N 1180005L1)

The OCU DP module is a single port access module used to provide the interface between a DS0 time slot on the T1 and a 4-wire DDS device at the customer premises. The OCU DP supports up to 18 kft of copper for remote DSU connectivity. This module is currently only supported by BCU L1 and L2.

## U-BR1TE Access Module (P/N 1180020L1)

The UBR1TE is a module that plugs into a single access slot of the Total Access 850. It provides an ISDN U-interface and allows transport of Basic Rate 2B+D information over T1 carriers and twisted pair wiring.

## E&M/TO Access Module (P/N 1180402L1)

The E&M/TO module is a single port Ear and Mouth/Transmit Only access module. The primary application for this module is to provide PBX foreign exchange at the customer premises or tandem central office applications. This module is intended for interface with intra-building wiring. The E&M/TO module supports both 2 and 4 wire operation. This module is currently only supported by BCU L1 and L2.

## Dual V.35 Access Module (P/N 1180025L1)

The Dual V.35 module is designed to provide additional V.35 interfaces for customer premises equipment. The module takes up two access slots; therefore three modules (six additional ports) can be added to an empty chassis. The Total Access 850 can support a maximum of seven V.35 interfaces. V.35 ports provided by the Dual V.35 module are accessed on the front of the Total Access 850. This module is currently only supported by the TDM version of the T1 RCU.

## DSX-1 Access Module (P/N 1200385L1)

The DSX-1 Module is a single port (RJ-45) access module that provides a DSX-1 connection for customer premises equipment. This module supports PBXs or other equipment with a DSX-1/FT1 interface.This module is currently supported by the T1 RCU only.

## Single DS0 DP Access Module (P/N 1180003L1)

The DS0 Dataport is a single port access module that serves as an interface to the basic DDS DSO (64 kbps) signal to a T-carrier line.This module is used in conjunction with an ADTRAN All-Rate Office Channel Unit (OCU) dataport or Total Reach DDS dataport located at the end office to extend the DDS network to an end office which has exclusively-served voice channels.

# ENGINEERING GUIDELINES

## CONTENTS

## FIGURES

## TABLES

## 1. EQUIPMENT DIMENSIONS

The Total Access 600 Series base unit is 8.5” W, 11” D, and 3.5” H and can be mounted in a 19-inch or 23-inch rack (mounting brackets included in shipment). All other equipment (modules) fit inside the base unit.

## 2. POWER REQUIREMENTS

Regardless of the configuration of access modules installed in the base unit, the following power requirements apply:

### AC System

90/130 VAC, 60 Hz, 50 Watt Max

### DC System

40/56 VDC, 50 Watt Max

## 3. REVIEWING THE FRONT PANEL DESIGN

Figure 1 shows the Total Access 600 Series front panel. Refer to *Access Module Interfaces* on page 31 for a discussion of available modules and the front panel functions of each.

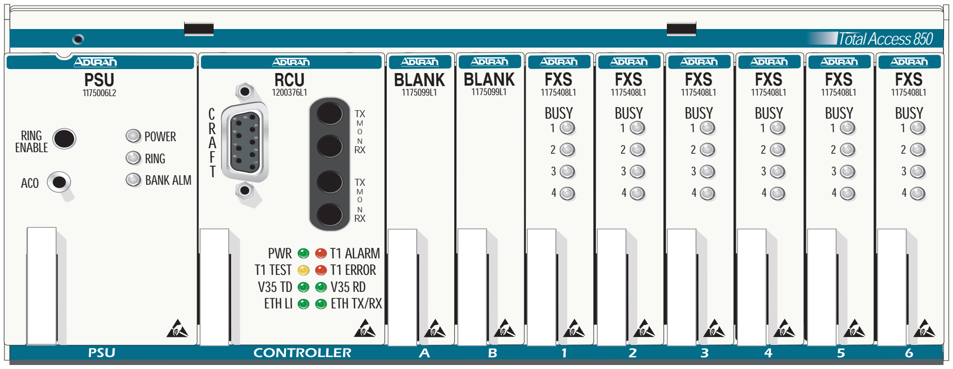


**Figure 1. Total Access 600 Series Front Panel Layout**

*UL 60950/NEBS requires all Total Access 600 Series empty slots to be covered with blank panels*
*(P/N 1175099L1).*

## LEDs

- PWR The RCU has power
- T1 ALARM There is an alarm on the network T1 (yellow, red, or blue alarm)
- T1 TEST The network T1 is in a test mode (loopback)
- T1 ERROR There are errors on the network T1 (framing errors, bipolar violations, or CRC errors)
- V35 TD There is transmit data detected on the V.35 port
- V35 RD There is receive data detected on the V.35 port
- ETH LI Ethernet link integrity
- ETH TX/RX There is transmit or receive data on the 10BaseT Ethernet port

## 4. REVIEWING THE REAR PANEL DESIGN

Figure 2 shows the Total Access 850 backplane and Table 1 gives the backplane connections.

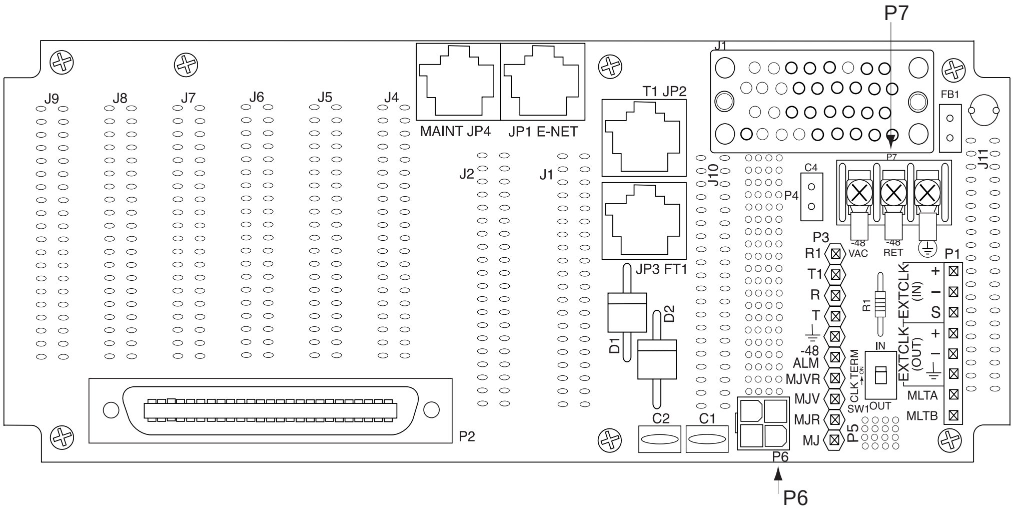


**Figure 2. Total Access 850 Rear Panel**

**Table 1. Total Access 850 Backplane Connections**

| Ref Des | Device/Label | Technology |
|---|---|---|
| P1 | wire-wrap strip | clock/tests |
| P2 | 50 pin amphenol | FXO, FXS, etc. |
| P3 | wire-wrap strip | alternate T1 interface |
| P5 | wire-wrap strip | alarms |
| P6 | 4 pin jack | primary -48 V in |
| P7 | 3-lug terminal | alternate -48 V in |
| JP1 | RJ-48/E-NET | 10BaseT Ethernet |
| JP2 | RJ-48/T1 | primary T1 interface |

| | | |
|---|---|---|
| JP3 | RJ-48/FT1 | DSX1 interface |
| JP4 | RJ-48/MAINT | RS 232 craft interface |
| J1 | V.35 | Nx56K/64K |

## 10BaseT Connection (JP1)

The 10BaseT port (RJ-48C) provides a 10BaseT Ethernet LAN connection, which is used for IP Routing, TFTP, SNMP, and Telnet connections. The network connection follows, and Table 2 shows the pinout.

| | |
|---|---|
| **CONNECTOR TYPE (USOC)** | RJ-48C |
| **PART NUMBER** | AMP# 555164-2 |

**Table 2. Ethernet Pinout**

| Pin | Name | Description |
|---|---|---|
| 1 | TX1 | Transmit Positive |
| 2 | TX2 | Transmit Negative |
| 3 | RX1 | Receive Positive |
| 4, 5 | UNUSED | — |
| 6 | RX2 | Receive Negative |
| 7, 8 | UNUSED | — |

## T1 Connection (JP2)

The MATRIX™ System provides a single T1 port (located on the rear panel) and complies with the applicable ANSI and AT&T™ standards. The T1 interface provides the following functions:

- AMI or B8ZS
- Manual line build-out
- D4 or ESF framing
- Network performance monitoring and reporting
- Test loopbacks with QRSS generation checking
- Extensive self-testing

The network connections follow, with the pinout shown in Table 3 below.

| | |
|---|---|
| **CONNECTOR TYPE (USOC)** | RJ-48C |

**Table 3. Network Connection Pinout**

| Pin | Name | Description |
|---|---|---|
| 1 | RXDATA-RING | Receive data from the network |
| 2 | RXDATA-TIP | Receive data from the network |
| 3 | UNUSED | — |
| 4 | TXDATA-RING | Transmit data toward the network |

| Pin | Name | Description |
|---|---|---|
| 5 | TXDATA-TIP | Transmit data toward the network |
| 6, 7, 8 | UNUSED | — |

## DSX-1 Connection (JP3)

The MATRIX™ System provides a single DSX-1 port (located in the rear of the unit) and complies with the applicable ANSI and AT&T™ standards. The DSX-1 interface provides the following functions:

- AMI or B8ZS
- Manual line build-out
- D4 or ESF framing

The network connections follow, with the pinout shown in Table 4.

**CONNECTOR TYPE (USOC)** RJ-48C

**Table 4. DSX-1 Network Connection Pinout**

| Pin | Name | | Description |
|---|---|---|---|
| 1 | R | TXDATA-RING | Transmit data from the network |
| 2 | T | TXDATA-TIP | Transmit data from the network |
| 3 | — | UNUSED | — |
| 4 | R1 | RXDATA-RING | Receive data toward the network |
| 5 | T1 | RXDATA-TIP | Receive data toward the network |
| 6, 7, 8 | — | UNUSED | — |

## Maint Port (JP4)

The Maint port (EIA-232) connects to a computer or modem. The control port input provides the following functions:

- Accepts EIA-232 input from a PC or a modem for controlling the Total Access 600 Series.
- Operates at 2400, 9600, 19200, or 38400 bps.
- Acts as input for either VT 100 or PC control.
- Acts as an interface for flash memory software downloads using XMODEM.

The Maint connection follows, and Table 5 shows the pinout.

| | |
|---|---|
| **CONNECTOR TYPE** | RJ-48C |
| **PART NUMBER** | AMP# 555164-2 |

**Table 5. Maint Pinout**

| Pin | Name | Description |
|---|---|---|
| 1 | GND | Ground - connected to unit chassis |
| 2 | RTS | Request to send - flow control |
| 3 | RXDATA | Data received by the Total Access 600 Series |
| 4 | DTR | Data terminal ready |
| 5 | TXDATA | Data transmitted by the Total Access 600 Series |
| 6 | CD | Carrier detect |
| 7 | UNUSED | — |
| 8 | CTS | Clear to send - flow control |

## Main Port (J1)

Each port of the Dual Nx56/64 Option Module has a V.35 Winchester-style connection as defined in the table below.

**Table 6. V.35 Winchester Pinout**

| Pin/CCIT | Description | Pin/CCIT | Description |
|---|---|---|---|
| A/101 | Protective ground (PG) | V/115 | RX clock (RC-A) to DTE |
| B/102 | Signal ground (SG) | X/115 | RX clock (RC-B) to DTE |
| C/105 | Request to send (RTS) from DTE | P/103 | Transmitted data (TD-A) from DTE |
| D/106 | Clear to send (CTS) to DTE | S/103 | Transmitted data (TD-B) to DTE |
| E/107 | Data set ready (DSR) to DTE | Y/114 | TX clock (TC-A) to DTE |
| E/109 | Data carrier detect | AA/114 | TX clock (TC-B) to DTE |
| H/— | Data terminal ready (DTR) from DTE | U/113 | External TX clock (ETC-A) from DTE |
| J/— | Ring indicator (RI) | W/113 | External TX clock (ETC-B) from DTE |
| R/104 | Received data (RD-A) to DTE | NN/— | Test mode (TM) to DTE |
| T/104 | Received data (RD-B) to DTE | | |

## Alarm Relay Connection (P5)

This connection alerts the user when a selected alarm condition exists. Alarm relay contacts are open during normal operation. The alarm relay contacts close in the event of a local alarm condition or the receipt of an alarm from the T1 carrier. In a carrier alarm condition such as a Red, Yellow, or Blue (unframed all 1s), various alarm contacts in the PSU close. Carrier alarm conditions cause the Total Access 850 to initiate trunk processing. The following chain of events then occur:

1. MJ will be directly shorted to MJR.
2. MJV will be directly shorted to MJVR.

Contacts MJ and MJR can be overridden manually during an alarm condition by pressing the ACO pushbutton on the PSU faceplate. If the 3-Amp power fuse on the PSU trips, the -48ALM relay will close, providing a -48 VDC signal on that pin. This alarm cannot be overridden by the ACO pushbutton. Refer to

Table 8 on page 29 for alarm notifications.

Table 7 shows the pinout for the Alarm Relay connector.

**Table 7. Alarm Relay Connector Pinout**

| Pin | Name | Description |
|---|---|---|
| 1 | -48 ALM | DC alarm output. |
| 2 | MJVR | Closes when a selected alarm condition is present. |
| 3 | MJV | Common connection between external circuitry and NC or NO terminal. |
| 4 | MJR | Major alarm audible common |
| 5 | MJ | Major alarm audible |

**Table 8. Alarm Notification**

| Alarm Condition | Relays Activated | | |
|---|---|---|---|
| | MJR | MJVR | -48 ALM |
| Red Alarm | X | X | |
| Yellow Alarm | X | X | |
| AIS Alarm | X | X | |
| PSU Power Fuse Fails | X | X | X |
| Alarms ACO Deactivates | X | X | |
| **Note**: ACO will not deactivate MJR after a power fuse failure. | | | |

## Customer Connection (P2)

One 50-pin female amphenol connector (P2) provides the interconnect wiring for the access modules located in slots 1 through 6 of the chassis. This connector is usually terminated with a punch-down block for premises wiring or connected directly to a cross-connect or main distribution frame. Figure 3 details the connector pinout.

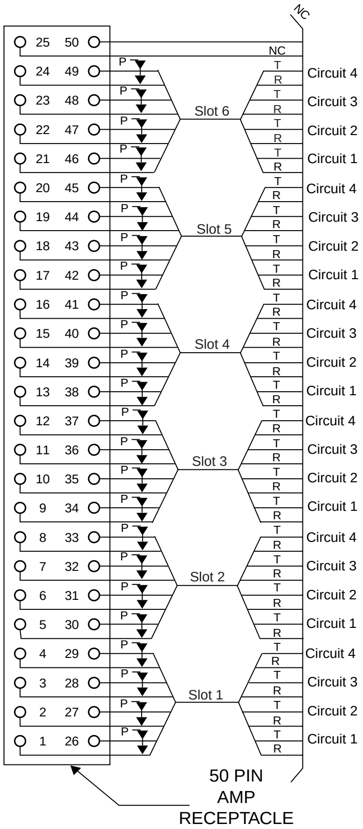


**Figure 3. Connector Pinout**

## T1 Wire-Wrap Connection (P3)

There are two termination points for connecting the network T1 to the chassis: the primary RJ-48 connector (JP2) and the alternate wire-wrap pins on terminal strip P3 (see Figure 2). Only one connector type is used (not both). The T1 primary connection is via the RJ-48 connector labeled T1 (JP2). This arrangement provides a convenient T1 connection for those installations where a T1 Smart Jack is used. Table 9 shows the pinout for the T1 wire-wrap connector.

**Table 9. T1 Wire-Wrap Connector Pinout**

| P3 Wire-Wrap Connections | | |
|---|---|---|
| Pin | Name | Description |
| 1 | R1 | DS1 Ring input from network |
| 2 | T1 | DS1 Tip input from network |
| 3 | R | DS1 Ring output from network |
| 4 | T | DS1 Tip output from network |
| 5 | Gnd | Ground |

## Power Connection (P6, P7)

There are two power connections on the backplane: a modular DC plug (P6), and a three lug terminal strip (P7) (refer to Figure 2). The primary connection is the modular plug, which receives -48 VDC from the ADTRAN power supply/battery charging unit (P/N 1175043L2). The alternate connection is screw terminal P7, which can be used if -48 VDC is available as in central office applications. The screw terminal connection is shown in Figure 4.

CAUTION

*During installation, power should be the last connection made after all other wire-wrap connections are completed.*

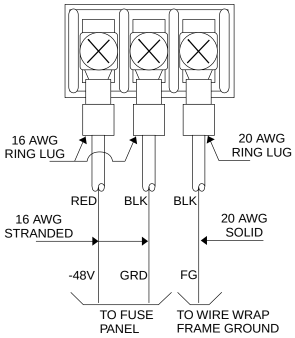


**Figure 4. Alternate Power Connection**

## 5. ACCESS MODULE INTERFACES

### Quad FXS and FXO Access Modules (P/N 1175408L2 and 1175407L2)

The Quad FXS and FXO Access Modules use the 50-pin female amphenol connector on the rear of the Total Access 850 chassis to provide the interconnect wiring for the four analog circuits on each access module. Figure 5 shows the pinout connection for the amphenol connector. See Figure 3 on page 30 for closer detail.

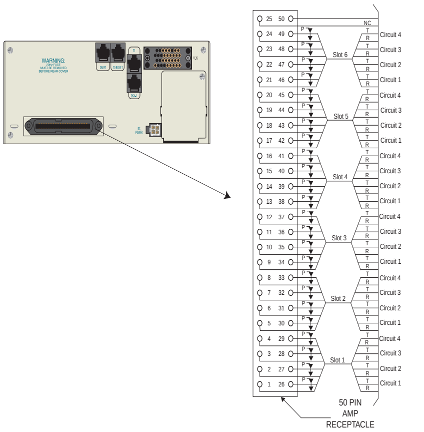


**Figure 5. Connector Pin Assignments**

## UBR1TE Access Module (P/N 1180020L1)

Each port of the UBR1TE Access Module provides an ISDN U-interface and allows the transport of Basic Rate 2B+D information over the T1 carrier and twisted pair wiring. Table 10 gives the pinout for this jack.

**CONNECTOR TYPE** (USOC) RJ-45

**Table 10. UBR1TE Pinout**

| Total Access 850 Slot | Port 1<br>T/R |
|---|---|
| 1 | 26/1 |
| 2 | 30/5 |
| 3 | 34/9 |
| 4 | 38/13 |
| 5 | 42/17 |
| 6 | 46/21 |

## OCU DP Access Module (P/N 1180005L1)

The OCU DP module is a single port access module used to provide the interface between a DS0 time slot on the T1 and a 4-wire DDS device at the customer premises. The OCU DP supports up to 18 kft of copper for remote DSU connectivity. This module is currently only supported by BCU L1 and L2. Table 11 gives this pinout.

**Table 11. OCU DP Pinout**

| Total Access 850 Slot | T/R RX | T1/R1 TX |
|---|---|---|
| 1 | 26/1 | 27/2 |
| 2 | 30/5 | 31/6 |
| 3 | 34/9 | 35/10 |
| 4 | 38/13 | 39/14 |
| 5 | 42/17 | 43/18 |
| 6 | 46/21 | 47/22 |

## E&M/TO Access Module (P/N 1180402L1)

The E&M/TO module is a single port Ear and Mouth/Transmit Only access module. The primary application for this module is to provide PBX foreign exchange at the customer premises or tandem central office applications. This module is intended for interface with intra-building wiring. The E&M/TO module supports both 2 and 4 wire operation. This module is currently only supported by BCU L1 and L2.

Table 12 gives the E&M/TO module pinout.

**Table 12. E&M/TO Pinout**

| | Slot 1 | Slot 2 | Slot 3 | Slot 4 | Slot 5 | Slot 6 | |
|---|---|---|---|---|---|---|---|
| Pin | 1 | 5 | 9 | 13 | 17 | 21 | RING |
| | 2 | 6 | 10 | 14 | 18 | 22 | RING 1 |
| | 3 | 7 | 11 | 15 | 19 | 23 | SG LEAD |
| | 4 | 8 | 12 | 16 | 20 | 24 | SB LEAD |
| | | | | | | | |
| Pin | 26 | 30 | 34 | 38 | 42 | 46 | TIP |
| | 27 | 31 | 35 | 39 | 43 | 47 | TIP 1 |
| | 28 | 32 | 36 | 40 | 44 | 48 | E LEAD |
| | 29 | 33 | 37 | 41 | 45 | 49 | M LEAD |

## Dual V.35 Access Module (P/N 1180025L1)

The Dual V.35 module is designed to provide additional V.35 interfaces for customer premises equipment. The module takes up two access slots; therefore three modules (six additional ports) can be added to an empty chassis. The Total Access 850 can support a maximum of seven V.35 interfaces. V.35 ports provided by the Dual V.35 module are accessed on the front of the Total Access 850. This module is currently only supported by the TDM version of the T1 RCU. An ADTRAN 35 ft DB-26/V.35 adapter cable is required (P/N 1200167L1). The pinout for the V.35 end of this cable is shown in Table 13.

**Table 13. Dual V.35 Pinout**

| Pin | Description |
|---|---|
| A | Frame ground |
| B | Signal ground |
| C | Request to send (RTS) |
| D | Clear to send (CTS) |
| E | Data set ready (DSR) |
| F | Received line signal detector (DCD) |
| H | Data terminal ready (DTR) |
| J | Ring indicator (RI) |
| K | unused |
| L | Local loopback (LL) |
| M | unused |
| N | unused |

**Table 13. Dual V.35 Pinout (Continued)**

| | |
|---|---|
| P | Transmitted data (TD-A) |
| R | Received data (RD-A) |
| S | Transmitted data (TD-B) |
| T | Received data (RD-B) |
| U | External TX clock (ETC-A) |
| V | RX clock (RC-A) |
| W | External TX clock (ETC-B) |
| X | RX clock (RC-B) |
| Y | TX clock (TC-A) |
| Z | unused |
| AA | TX clock (TC-B) |
| BB | unused |
| CC | unused |
| DD | unused |
| EE | unused |
| FF | unused |
| HH | unused |
| JJ | unused |
| KK | unused |
| LL | unused |
| MM | unused |
| NN | Test mode (TM) |

## DSX-1 Access Module (P/N 1200385L1)

The DSX-1 Module is a single port (RJ-45) access module that provides a DSX-1 connection for customer premises equipment. This module supports PBXs or other equipment with a DSX-1/FT1 interface. This module is currently supported by the T1 RCU only.

**Table 14. DSX-1 Pinout**

| Pin | Name | Description |
|---|---|---|
| 1 | R1 \| RXDATA-RING | Receive data from the network (RING) |
| 2 | T1 \| RXDATA-TIP | Receive data from the network (TIP) |
| 3 | UNUSED | — |
| 4 | R \| TXDATA-RING | Transmit data towards the network (RING) |
| 5 | T \| TXDATA-TIP | Transmit data towards the network (TIP) |
| 6,7,8 | UNUSED | — |

# NETWORK TURNUP PROCEDURE

## CONTENTS

## FIGURES

## 1. INTRODUCTION

This section discusses the installation process of the Total Access 850 installation.

## 2. TOOLS REQUIRED

The tools required for wallmount installation of the Total Access 850 shelf are:

- Four #8 x 3/4 inch pan-head wood screws
- Drill and drill bit set
- Flat head screwdriver (medium)
- Two Phillips head screwdrivers (small /medium)
- Wire-wrap gun (optional)
- 5-pair male amphenol cable (customer connection)
- Selected punch-down block and tool

WARNING *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION *During installation, power should be the last connection made.*

CAUTION *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.*

## 3. UNPACK AND INSPECT THE SYSTEM

Each Total Access 850 is shipped in its own cardboard shipping carton. Open each carton carefully and avoid deep penetration into the carton with sharp objects.

After unpacking the unit, inspect it for possible shipping damage. If the equipment has been damaged in transit, immediately file a claim with the carrier, then contact ADTRAN Customer Service (see *Customer Service, Product Support Information, and Training* in the front of this manual).

## Contents of ADTRAN Shipments

Your ADTRAN shipment of the Total Access 850 chassis includes the following items:

- The Total Access 850 Base Unit
- The Total Access 850 Family System CD
- Wallmount brackets and screws
- RJ-45 to RJ-45 8-pin cable (15 ft) - ADTRAN P/N 3125M008
- UL 1950 Notice Card - ADTRAN P/N 61200375L1-17
- Manual Ordering Information Notice Card - ADTRAN P/N 61200375L1-1702

CAUTION *Customer must supply Ethernet cable.*

## 4. GROUNDING INSTRUCTIONS

To following provides grounding instruction information from the Underwriters' Laboratory UL1950 Standard for Safety of Information Technology Equipment Including Electrical Business Equipment, of July 28, 1995.

An equipment grounding conductor that is not smaller in size than the ungrounded branch-circuit supply conductors is to be installed as part of the circuit that supplies the product or system. Bare, covered, or insulated grounding conductors are acceptable. Individually covered or insulated equipment grounding conductors shall have a continuous outer finish that is either green, or green with one or more yellow stripes. The equipment grounding conductor is to be connected to ground at the service equipment.

The attachment-plug receptacles in the vicinity of the product or system are all to be of a grounding type, and the equipment grounding conductors serving these receptacles are to be connected to earth ground at the service equipment.

A supplementary equipment grounding conductor shall be installed between the product or system and ground that is in addition to the equipment grounding conductor in the power supply cord.

The supplementary equipment grounding conductor shall not be smaller in size than the ungrounded branch-circuit supply conductors. The supplementary equipment grounding conductor shall be connected to the product at the terminal provided, and shall be connected to ground in a manner that will retain the ground connection when the product is unplugged from the receptacle. The connection to ground of the supplementary equipment grounding conductor shall be in compliance with the rules for terminating bonding jumpers at Part K or Article 250 of the National Electrical Code, ANSI/NFPA 70. Termination of the supplementary equipment grounding conductor is permitted to be made to building steel, to a metal electrical raceway system, or to any grounded item that is permanently and reliably connected to the electrical service equipment ground.

The supplemental grounding conductor shall be connected to the equipment using a number 8 ring terminal and should be fastened to the grounding lug provided on the rear panel of the equipment. The ring terminal should be installed using the appropriate crimping tool (AMP P/N 59250 T-EAD Crimping Tool or equivalent.)

## 5. SUPPLYING POWER TO THE UNIT

### AC Powered Systems

The AC powered Total Access 850 (requires the use of the AC Power supply unit P/N 1175043L2) comes equipped with a 6-foot power cord with a 3-prong plug for connecting to a grounded power receptacle. As shipped, the Total Access 850 is set to factory default conditions. After installing the chassis and any access modules, the Total Access 850 is ready for power-up. To power-up the unit, ensure that the unit is properly connected to an appropriate power source.

CAUTION

- *This unit shall be installed in accordance with Article 400 and 364.8 of the NEC NFPA 70 when installed outside of a Restricted Access Location (i.e., central office, behind a locked door, service personnel only area).*
- *Power to the Total Access 850 AC system must be from a grounded 90-130 VAC, 50/60 Hz source.*
- *The power receptacle uses double-pole, neutral fusing.*
- *Maximum recommended ambient operating temperature is 45 ºC.*

### DC Powered Systems

The DC powered Total Access 850 comes equipped with a DC Power supply to furnish the voltages necessary for proper backplane operation. As shipped, the Total Access 850 is set to factory default conditions. After installing the chassis and any access modules, the Total Access 850 is ready for power-up.

CAUTION

- *This unit shall be installed in accordance with Article 400 and 364.8 of the NEC NFPA 70 when installed outside of a Restricted Access Location (i.e., central office, behind a locked door, service personnel only area).*
- *Power to the Total Access 850 DC system must be from a reliably grounded -48 VDC source which is electrically isolated from the AC source.*
- *The branch circuit overcurrent protection shall be a fuse or circuit breaker rated minimum 48 VDC, maximum 20A.*
- *Maximum recommended ambient operating temperature is 45 $^{o}$C.*

## 6. MOUNTING OPTIONS

The Total Access 850 chassis may be wallmounted or installed in a 19-inch or 23-inch rack. Wallmount brackets are included with the chassis. For a rackmount installation, the Total Access 850 Base Unit allows flush-face mount, face-forward mount, center mount, and rear mount.

NOTE

*The Total Access 850 chassis includes wall mount brackets. If rack mount brackets are needed, use part number 1175045L1 or 1175046L1 for 19 inch or 23 inch, respectively.*

CAUTION

*Be careful not to upset the stability of the equipment mounting rack when installing this product.*

## 7. INSTALLING ACCESS MODULES

Figure 1 shows the slot numbering designation as viewed from the front of the Total Access 850 chassis. The functionally identical option slots only accept Total Access™ access modules and the controller slots only accept Total Access 850 controller modules.

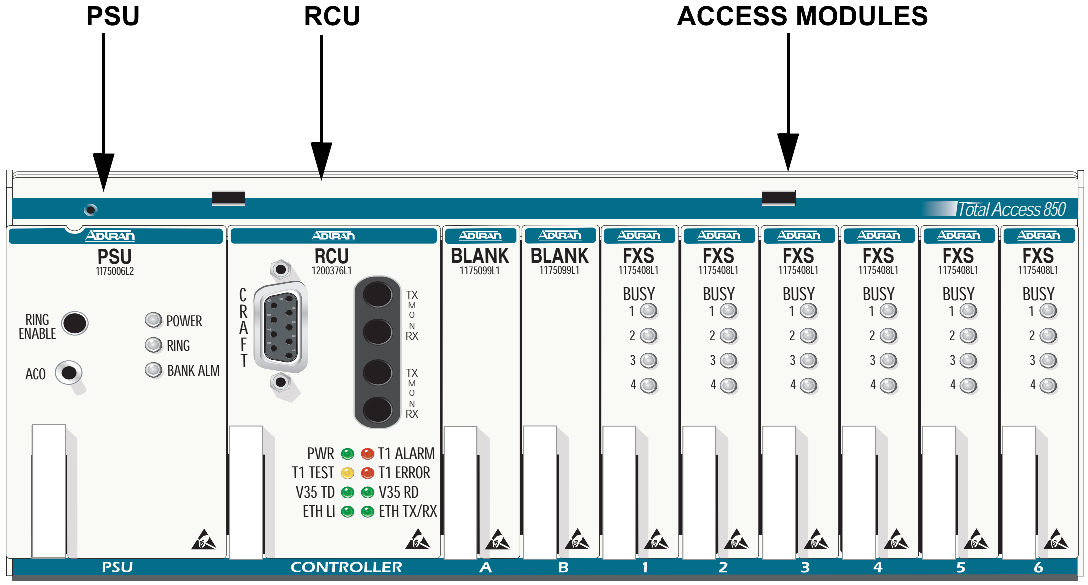


**Figure 1. Total Access 850 Slot Designation (Front View)**

WARNING

*Access modules are intended to be serviced by qualified service personnel only.*

## Instructions for Installing the Total Access 850 Controller Resource and Access Modules

Individual access modules insert from the front. A locking bar holds the modules in place for added security. Disengaging the captured screw allows removal of the locking bar. To install Controller Resource and Access Modules for the Total Access 850, follow the steps outlined below.

1. Hold the access module by the faceplate while supporting the bottom side.
2. Align the module edges to the guide grooves for the designated slot.
3. Insert the module until the edge connector seats firmly into the backplane.
4. Lock the module in place by pushing in on the locking lever.
5. Connect the cables to the associated device(s). All wiring connections terminate on the backplane of the chassis.

> **WARNING**
>
> *Disable ring voltage before exposing the backplane or accessing channel units. For the L2 PSU, press the Ring Enable button. For older L1 PSUs, remove the 20 Hz fuse.*

### Quad FXO Access Module (P/N 1175407L2)

#### *Shipping Contents*

The ADTRAN shipment of the Quad FXO Access Module includes the following items:

- Quad FXO Access Module
- Quad FXO Access Module Job Aid
- Quad FXS/FXO Compliance Sheet

### Quad FXS Access Module (P/N 1175408L2)

#### *Shipping Contents*

The ADTRAN shipment of the Quad FXS Access Module includes the following items:

- Quad FXS Access Module
- Quad FXS Access Module Job Aid
- Quad FXS/FXO Compliance Sheet

## UBR1TE Access Module (P/N 1180020L1)

### *Shipping Contents*

The ADTRAN shipment of the UBR1TE Access Module includes the following items:

- UBR1TE Access Module
- UBR1TE Access Module Job Aid

## OCU DP Access Module (P/N 1180005L1)

### *Shipping Contents*

The ADTRAN shipment of the OCU DP Access Module includes the following items:

- OCU DP Access Module
- OCU DP Access Module Job Aid

## E&M/TO Access Module (P/N 1180402L1)

### *Shipping Contents*

The ADTRAN shipment of the E&M/TO Access Module includes the following items:

- E&M/TO Access Module
- E&M/TO Access Module Job Aid

## Dual V.35 Access Module (P/N 1180025L1)

### *Shipping Contents*

The ADTRAN shipment of the Dual V.35 Access Module includes the following items:

- Dual V.35 Access Module
- Dual V.35 Access Module Job Aid

## DSX-1 Module (P/N 1200385L1)

The ADTRAN shipment of the DSX-1 Module includes the following items:

- DSX-1 Module
- DSX-1 Module Installation and Maintenance Practice

# SECTION 4.0 COMMONS USER INTERFACE GUIDE

This section of the Total Access 850 System Manual is designed for use by network administrators and others who will configure and provision the system. It contains information about navigating the VT100 user interface, configuration information, and menu descriptions.

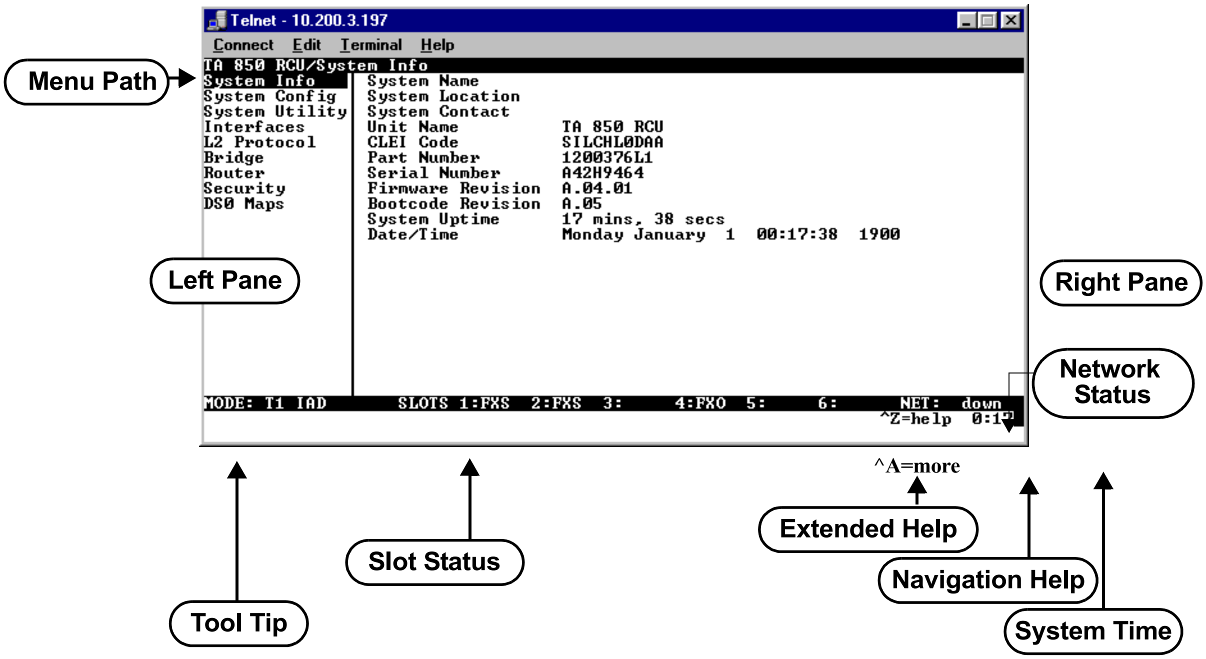
## CONTENTS

## FIGURES

# 1. NAVIGATING THE TERMINAL MENU

## Terminal Menu Window

The Total Access 850 uses a multi-level menu structure that contains both menu items and data fields. All menu items and data fields display in the terminal menu window (see Figure 1), through which you have complete control of the Total Access 850.



```
TA 850 RCU/System Info
System Info     System Name
System Config   System Location
System Utility  System Contact
Interfaces      Unit Name          TA 850 RCU
L2 Protocol     CLEI Code          SILCHL0DAA
Bridge          Part Number        1200376L1
Router          Serial Number      A42H9464
Security        Firmware Revision  A.04.01
DS0 Maps        Bootcode Revision  A.05
                System Uptime      17 mins, 38 secs
                Date/Time          Monday January  1  00:17:38  1900

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:    4:FXO  5:     6:      NET:  down
                                                               ^Z=help  0:1
```

**Figure 1. Top-Level Terminal Menu Window**

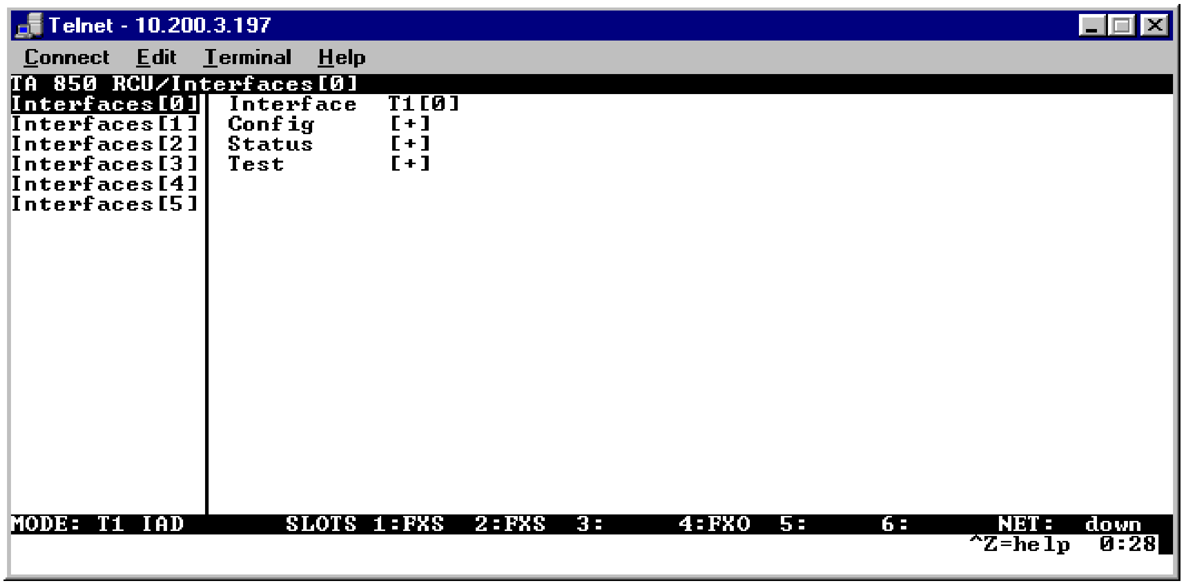
### *Menu Path*

The first line of the terminal menu window (the menu path) shows the session's current position (path) in the menu structure. For example, Figure 1 shows the top-level menu with the cursor on the **SYSTEM INFO** submenu; therefore, the menu path reads **TA 850 RCU > System Info**.

## *Window Panes*

When you first start a terminal menu session, the terminal menu window is divided into left and right panes. The left pane shows the list of available submenus, while the right pane shows the contents of the currently selected submenu.

You can view the terminal windows in two ways: with fields and submenus displaying horizontally across the right pane, or with fields and submenus displaying vertically down the right pane. Viewing submenus vertically rather than horizontally allows you to see information at a glance rather than scrolling horizontally across the window. To change the view, move your cursor to an index number and press **<Enter>**. Figure 2 shows this alternate view. Fields and submenu names may vary slightly in this view.



```
TA 850 RCU/Interfaces[0]
Interfaces[0]  Interface   T1[0]
Interfaces[1]  Config      [+]
Interfaces[2]  Status      [+]
Interfaces[3]  Test        [+]
Interfaces[4]
Interfaces[5]

MODE: T1 IAD        SLOTS 1:FXS  2:FXS  3:      4:FXO  5:      6:       NET:  down
                                                                      ^Z=help  0:28
```

**Figure 2. Alternate Menu View**

### Window Pane Navigation

Use the following chart to assist you in moving between and within the two window panes.

| To do this... | Press this key... |
|---|---|
| Move from left pane to right pane | Tab<br>Enter<br>Right arrow |
| Move from right pane to left pane | Tab<br>Escape<br>Left arrow<br>Backspace |
| Move within each pane | Up arrow<br>Down arrow<br>Left arrow<br>Right arrow |

### Right Window Pane Notation

The right window pane shows the contents of the currently selected menu. These contents can include both submenu items and data fields. Some submenus contain additional submenus and some data fields contain additional data fields. The following chart explains the notation used to identify these additional items.

| This notation... | Means that... |
|---|---|
| [+] | More items are available when selected |
| <+> | An action is to be taken, such as activating a test |
| Highlighted menu item | You can enter data in this field |
| Underlined field | The field contains read-only information |

## *Additional Terminal Menu Window Features*

- Tool Tip - provides a brief description of the currently selected mode
- Network Status - displays network status information, Up or Down
- Slot Status - displays type of module installed in each slot. No entry will appear for slots not containing a module.
- Extended Help - displays information about selected commands (CTRL+A)
- Navigation Help - lists characters used for navigating the terminal menu and session management (CTRL+Z)
- System Time - displays current time

## Navigating using the Keyboard Keys

You can use various keystrokes to move through the terminal menu, to manage a terminal menu session, and to configure the system. Press <CTRL+Z> to activate a pop-up screen listing the navigation keystrokes.

### *Moving through the Menus*

| **To do this...** | **Press this key...** |
|---|---|
| Return to the home screen | H |
| Jump between two menu items<br>Press <J> while the cursor is located on a menu item, and you jump back to the main screen.<br>Go to another menu item, press <J>, and you jump back to the screen that was displayed the first time you pressed <J>.<br>Press <J> anytime you want to jump between these items. | J |
| Select items | Arrows |
| Edit a selected menu item | Enter |
| Cancel an edit | Escape |
| Close pop-up help screen | Escape |
| Move between the left and right panes | Tab<br>Arrows |
| Move to the top of a screen | A |
| Move to the bottom of a screen | Z |
| Ascend one menu level | Backspace |
| Jump to terminal mode (only supported in T1 TDM code) | Ctrl + T |
| Jump to NAT menu (only supported in T1 TDM code) | Ctrl + N |

## *Session Management Keystrokes*

| **To do this...** | **Press this key...** |
|---|---|
| Log out of a session | CTRL+L |
| Refresh the screen<br>To save time, only the portion of the screen that has changed is refreshed. This option should only be necessary if the display picks up incorrect characters. | CTRL+R |

## *Configuration Keystrokes*

| **To do this...** | **Press this key...** |
|---|---|
| Restore factory default settings.<br>This setting restores the factory defaults based on the location of the cursor. If the cursor is on a module line (in the **MODULES** menu), then only the selected module is updated to factory defaults. | F |
| Copy selected items to the clipboard.<br>The amount of information you can copy depends on the cursor location when you press <C>:<br>If the cursor is over an editable field, only that item is copied.<br>If the cursor is over the index number of a list, then all of the items in the row of the list are copied. For example, if the cursor is over the **SLOT #** field in the **MODULES** screen, all of the information associated with the slot is copied. | C |
| Paste the item stored in the clipboard, if the information is compatible.<br>You must confirm all pastes - except those to a single editable field. | P |
| Increment the value of certain types of fields by one when you paste information into those fields. | > |
| Decrement the value of certain types of fields by one when you paste information into those fields. | < |

| To do this... | Press this key... |
|---|---|
| Insert a new list item.<br>For example, add a new item to the **TELNET USER LIST** connection list by pressing <I> while the cursor is over the index number. | I |
| Delete a list item.<br>For example, delete an item from the **TELNET USER LIST** connection list by pressing <D> while the index number is active. | D |

### *Getting Help*

The bottom line of the terminal menu window contains context-sensitive help information. When the cursor is positioned over a set of configuration items, a help message displays (when available) providing a description of the item. When more detailed help is available for a particular item, **^A** displays at the bottom of the window. At this point, if you press <CTRL+A>, a pop-up help screen displays with information about the item.

Press <CTRL+Z> to activate a help screen that displays the available keystrokes you can use to navigate the terminal menu. Press <Esc> to cancel these pop-up windows.

## 2. TERMINAL MENU AND SYSTEM CONTROL

### Selecting the Appropriate Menu

The terminal menu is the access point to all other operations. Each terminal menu item has several functions and submenus that identify and provide access to specific operations and parameters. Use the chart below to help select the appropriate terminal menu.

| To do this... | Go to this menu... |
|---|---|
| Review and monitor general system information for the Total Access 850 | **SYSTEM INFO** |
| Set up the operational configuration for the Total Access 850 | **SYSTEM CONFIG** |
| Upgrade firmware, do config transfers, ping, and access terminal mode | **SYSTEM UTILITY** |
| Define, configure, and monitor all Total Access 850 Router functions | **ROUTER** |
| Review and configure settings for each installed module, configure the DS0 maps, and configure the V.35 parameters | **CHANNEL BANK** |

## Security Levels

To edit terminal menu items, you must have a password and the appropriate security level. Table 1 describes the security levels.

**Table 1. Password Security Level**

| Security Level | Description |
|---|---|
| Status | Read-only permission for all menu items - **minimum rights** |
| Voice | Read permission for all menu items and permission to use test commands |
| Router | Access to all commands except passwords, flash download, authentication methods, interface configurations, and telnet security levels |
| Config | Access to all commands except passwords, flash download, authentication methods, and telnet security levels |
| Support | Access to all commands except passwords and telnet security levels |
| Full | Permission to edit every menu item, including creating and editing passwords - **maximum rights** |
| Router only | Read access to all menus and write access to only the router menu |

## 3. ACCESS MODULE MENU DESCRIPTIONS

> NOTE *The following Access Module Menu Descriptions section only applies to Total Access 850 systems with firmware versions prior to the A.04 or C.04 code releases. Refer to the individual technology based User Interface Guides (T1 TDM and ATM) for a detailed discussion of the newer menu selections.*

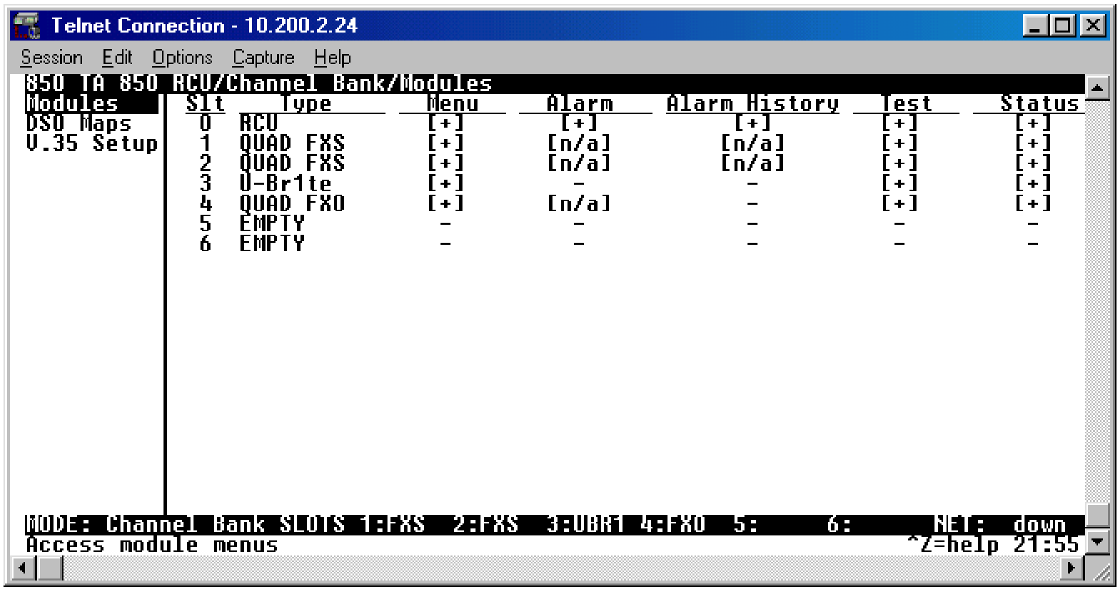
This section describes the Total Access 850 FXO, UBR1TE, and FXS menu and submenu options. Refer to the other User Interface Guides in this manual for detailed information on other Total Access 850 menus and submenus.

### CHANNEL BANK MENUS

Access the FXO, UBR1TE, and FXS menus through the **CHANNEL BANK** menu, which provides access to the module configuration, DS0 maps, and V.35 setup.

### CHANNEL BANK > MODULES

Use the **CHANNEL BANK > MODULES** menu to view and set the parameters shown in Figure 3 on page 51 for the FXO, UBR1TE, and FXS modules.


Telnet Connection - 10.200.2.24
Session Edit Options Capture Help

```
850 TA 850 RCU/Channel Bank/Modules
Modules      Slt    Type        Menu     Alarm    Alarm History   Test     Status
DS0 Maps      0   RCU           [+]       [+]         [+]          [+]      [+]
V.35 Setup    1   QUAD FXS      [+]      [n/a]       [n/a]         [+]      [+]
              2   QUAD FXS      [+]      [n/a]       [n/a]         [+]      [+]
              3   U-Br1te       [+]       -           -            [+]      [+]
              4   QUAD FXO      [+]      [n/a]        -            [+]      [+]
              5   EMPTY          -        -           -             -        -
              6   EMPTY          -        -           -             -        -

MODE: Channel Bank SLOTS 1:FXS  2:FXS  3:UBR1 4:FXO  5:    6:      NET:  down
Access module menus                                           ^Z=help 21:55
```

Figure 3. Channel Bank > Modules Menu

## QUAD FXO MODULE MENUS

### CHANNEL BANK > MODULES > MENU

Displays the configuration options for the selected module. To access the submenus for this item, use the arrow keys to scroll to the menu column for the module you want to edit and press enter.

### CHANNEL BANK > MODULES > TYPE

Displays the type of module installed in the slot. The Total Access 850 automatically detects the type of module installed in each slot, and the TYPE field displays the module name. This is a read-only field.

NOTE *If a module is installed, the module type automatically shows the name of the installed module, and it cannot be set to any other option.*

NOTE *If a module is removed while the unit is powered on, the module options will not change until a new module type is installed or power is cycled.*

### CHANNEL BANK > MODULES > MENU > MODE

Choices are **LOOP START, GROUND START,** and **DPT**. Default is **LOOP START.**

**LOOP START -** Sets the port to use FXO loop start signaling on the T-span and loop start supervision on the analog 2-wire interface.

**GROUND START -** Sets the port to use FXO ground start signaling on the T-span and ground start supervision on the analog 2-wire interface.

**DPT -** Sets the port to use Dial Pulse signaling to terminate dialed numbers.

NOTE *This mode needs to be set based on how the network is set up and how each port is being used. Each port does not need to be set to the same mode.*

### CHANNEL BANK > MODULES > MENU > TX (dB)

Sets the TX direction level points. The value entered must be less than 10 dB. Default is **0.0 dB**.

### CHANNEL BANK > MODULES > MENU > RX (dB)

Sets the RX direction level points. The value entered must be less than 10 dB. Default is **0.0 dB**. The **0.0 dB** setting is the strongest signal. The **10.0 dB** setting adds attenuation.

### CHANNEL BANK > MODULES > MENU > SVC MODE

Indicates whether the module is **IN SERVICE** or **OUT OF SVC**. This does not indicate whether the port has been mapped. For proper operation, the port must be mapped using the **DS0 MAPS** menu. Default is **IN SERVICE.**

### CHANNEL BANK > MODULES > ALARM (N/A)

### CHANNEL BANK > MODULES > ALARM HISTORY (N/A)

### CHANNEL BANK > MODULES > TEST > TEST

To initiate a module test, scroll to the **TEST** column and press enter. The choices (described below) are **NONE, DIGITAL NET LPBK, NETWORK ON HOOK TEST, NETWORK OFF HOOK TEST, 1 KHZ TONE-NEAR END,** and **1 KHZ TONE-FAR END.** Default is **NONE.**

**NONE -** Indicates that no test is currently active.

**DIGITAL NET LPBK -** Used to loop back DS0 data coming from the network for each channel. Received data is latched in on the appropriate receive time slot on the receive bus. This data is then placed on the transmit bus in the unit's transmit time slot.

**NETWORK ON-HOOK TEST -** Used to test signaling sent to the network by the unit. On-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

**NETWORK OFF-HOOK TEST -** Used to test signaling sent to the network by the unit. Off-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

**1 KHZ TONE-NEAR END** - This test option is only applicable for FXO and FXS modules. For Near End, the 2-wire side sends out a 1 kHz tone to verify talk path. (In the BCU, this tone option is bidirectional and can be heard at the Near End as well as the Far End.)

**1 KHZ TONE-FAR END** - This test option is only applicable for FXO and FXS modules. For Far End, the tone side is sent out across the Network and can be heard if monitoring on the T1 as well as off of the far-end 2-wire side. Again, this verifies talk path. (In the BCU, this tone option is bidirectional and can be heard at the Near End as well as the Far End.)

### CHANNEL BANK > MODULES > TEST > TEST STATUS

Displays whether a test is in progress.

### CHANNEL BANK > MODULES > STATUS > TA SIG

This parameter displays the status of the Transmit A signal bit. The high/low status is indicated by a 0 or 1.

### CHANNEL BANK > MODULES > STATUS >TB SIG

This parameter displays the status of the Transmit B signal bit. The high/low status is indicated by a 0 or 1.

### CHANNEL BANK > MODULES > STATUS > RA SIG

This parameter displays the status of the Receive A signal bit. The high/low status is indicated by a 0 or 1.

### Channel Bank > Modules > Status > RB Sig

This parameter displays the status of the Receive B signal bit. The high/low status is indicated by a 0 or 1.

## UBR1TE Module Menus

### Channel Bank > Modules > Menu

Displays the configuration options for the selected module. To access the submenus for this item, use the arrow keys to scroll to the menu column for the module you want to edit and press enter.

### Channel Bank > Modules > Type

Displays the type of module installed in the slot. The Total Access 850 automatically detects the type of module installed in each slot, and the TYPE filed displays the module name. This is a read-only field.

> NOTE *If a module is installed, the module type automatically shows the name of the installed module, and it cannot be set to any other option.*

> NOTE *If a module is removed while the unit is powered on, the module options will not change until a new module type is installed or power is cycled.*

### Channel Bank > Modules > Menu > Mode

Choices are **Lunt, Lunt w/Wakeup,** and **Lult**. The U-BR1TE port should be configured to operate in the **LULT** mode if being operated in the Adjacent to Customer or Tandem Office Source positions (see Figure 4 on page 55). The **MODE** should be set to **LUNT** if the port is operated in the Adjacent to Switch or

Tandem Office Sink positions. Default is **LULT.**

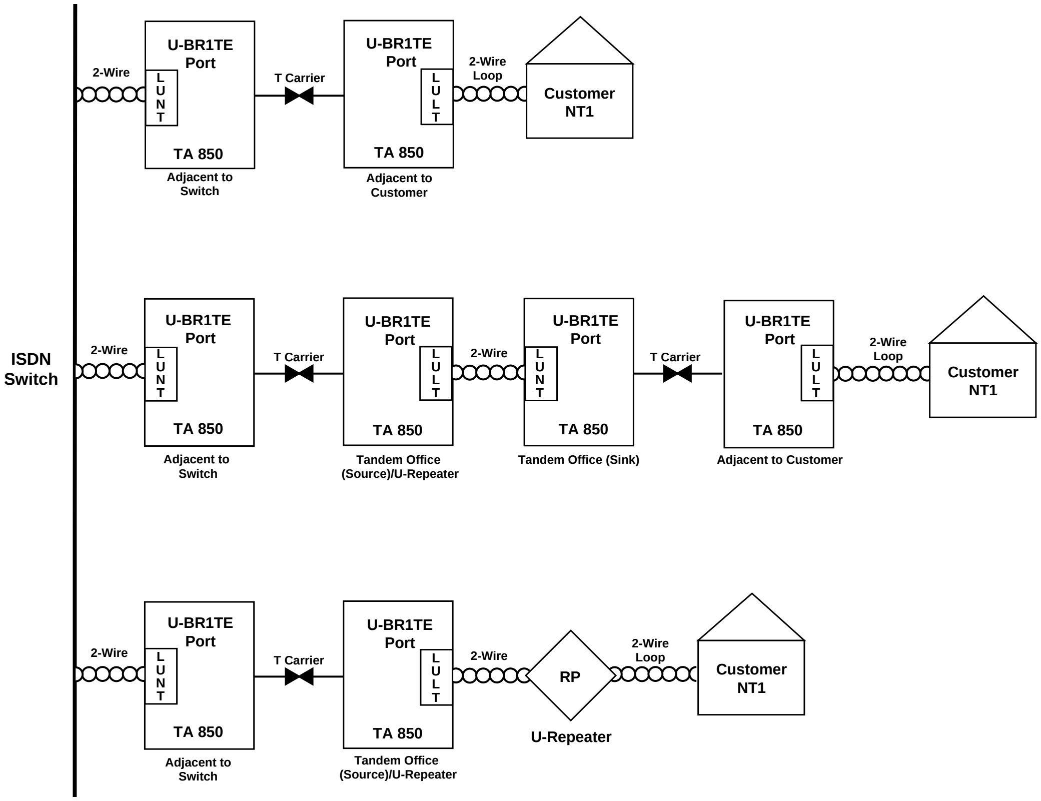


**Figure 4. Network Locations**

## CHANNEL BANK > MODULES > MENU > SERVICE

SERVICE allows the user to select the ISDN channels to be transmitted over the T1 facility. Each channel requires one DS0 of the T1 in which to transmit and receive data. All switched applications will require the D channel. Choices are **2B+D, B1+D, B2+D, B1+B2, B1, B2,** and **D**. Default is **2B+D.**

NOTE *The user must provision the proper number of consecutive DS0s of the T1 facility for proper operation.*

## CHANNEL BANK > MODULES > MENU > ZERO BYTE SUB

For proper operation, the **ZBS** (zero byte substitution) for two U-BR1TE ports connected by a T1 facility must be the same value. The **ENABLE** parameter for **ZBS** must be selected if the T1 is using AMI line coding. If the T1 facility is using B8ZS line coding, the **DISABLE** parameter may be chosen. Default is **ENABLED.**

### CHANNEL BANK > MODULES > MENU > SEALING CURRENT

This option is only applicable if the Module is a UBrite card. DC sealing current is only applicable if the mode is **LULT**. Sealing current should be present for Adjacent-to-Customer applications. Default is **ENABLED.**

### CHANNEL BANK > MODULES > ALARM

Depending upon the modules housed in slots 1-6, the alarm reporting conditions will vary. For slot 0 RCU, Alarm will report LOS, RED, YELLOW, and BLUE alarms for both port 1 (Network) and port 2 (DSX). Alarms are not reported for the DSX if no channels are mapped to the port.

### CHANNEL BANK > MODULES > ALARM HISTORY

Only applicable for the RCU module. This is a history latch that comes on if the unit has reported any alarming conditions since the last time it was cleared. The clear history button will clear these alarms in the history.

### CHANNEL BANK > MODULES > TEST > B-CHANNEL

Select the channel to be placed in test (channel 1 or 2).

### CHANNEL BANK > MODULES > TEST > TEST CHANNEL

This is only an option if the module is a UBR1TE card. Choices are **NONE, ADDR1 (LOCAL LPBK), ADDR2, ADDR3, ADDR4, NT1, TX INTO CARRIER, TX INTO LOOP,** and **BILATERAL LPBK**. Default is **NONE.**

### CHANNEL BANK > MODULES > STATUS > ACT BIT

This status field indicated whether an NT1 is communicating with the ISDN switch.

### CHANNEL BANK > MODULES > STATUS > LOOP

This status screen indicates whether synchronization exists between the UBR1TE card and the NT1 on the loop side of the card. Sync will display Yes or No.)

### CHANNEL BANK > MODULES > STATUS > CARRIER

This status screen indicates whether synchronization exists between the ISDN switch and the UBR1TE card on the T1. Sync will display Yes or No.

### CHANNEL BANK > MODULES > STATUS > RX LOOP

Again, this is ONLY an option if the module is a UBR1TE card. If the ISDN line is in sync across the network, **RX LOOP** will be **YES**.

## QUAD FXS MODULE MENUS

### CHANNEL BANK > MODULES > MENU

Displays the configuration options for the selected module. To access the submenus for this item, use the arrow keys to scroll to the menu column for the module you want to edit and press enter.

### CHANNEL BANK > MODULES > TYPE

Displays the type of module installed in the slot. The Total Access 850 automatically detects the type of module installed in each slot, and the TYPE filed displays the module name. This is a read-only field.

*If a module is installed, the module type automatically shows the name of the installed module, and it cannot be set to any other option.*

*If a module is removed while the unit is powered on, the module options will not change until a new module type is installed or power is cycled.*

### CHANNEL BANK > MODULES > MENU > MODE

Choices are given below. Default is **LOOP START.**

*This mode needs to be set based on how the network is set up and how each port is being used. Each port does not need to be set to the same mode.*

**LOOP START -** Sets the port to use FXS loop start signaling on the T-span and loop start supervision on the analog 2-wire interface.

**GROUND START -** Sets the port to use FXS ground start signaling on the T-span and ground start supervision on the analog 2-wire interface.

**TR08 SINGLE -** Sets the port to use Single Party Channel Unit signaling on the T-span (as defined by TR-TSY-000008) and loop start supervision on the analog 2-wire interface.

**TR08 UVG -** Sets the port to use Universal Voice Grade signaling on the T-span (as defined by TR-TSY-000008) and either loop start or ground start supervision on the analog 2-wire interface.

**DPO -** Sets the port to use Dial Pulse signaling to originate dialed numbers.

**TANDEM (E&M) -** Sets the port to use E&M signaling on the T-span and either loop start or ground start supervision on the analog 2-wire interface. See the Tandem submenus for more information.

### CHANNEL BANK > MODULES > MENU > TX (DB)

Sets the TX direction level points. The value entered must be less than 10 dB. Default is **6.0 dB**. 0.0. dB is the maximum signal. dB is in attenuation.

### CHANNEL BANK > MODULES > MENU > RX (DB)

Sets the RX direction level points. The value entered must be less than 10 dB. Default is **3.0 dB**. 0.0. dB is the maximum signal. dB is in attenuation.

### CHANNEL BANK > MODULES > MENU > SVC MODE

Indicates whether the module is **IN SERVICE** or **OUT OF SVC**. This does not indicate whether the port has been mapped. For proper operation, the port must be mapped using the **DS0 MAPS** menu. Default is **IN SERVICE.**

### CHANNEL BANK > MODULES > MENU > LINE Z

Sets the line impedance. Choices are **600 OHMS**, **900 OHMS**, **600 OHMS + 2.16μF**, **900 OHMS + 2.16 μF**, and **AUTO**. The line impedance of each port is based on the size of the network. Default is **600 OHMS.**

### CHANNEL BANK > MODULES > MENU > MSG IND

This is only an option under the FXS menu for the Message Indicating. This is better referred to as On-Hook Message Waiting. When this is set to **ENABLE**, talk path is always open, even in On-Hook conditions, in order for these FXS message tones to pass through. Default is **DISABLE.** Enabling the message lamp will allow message lamp usage but will cause a lower on-hook voltage. Disabling this feature will allow higher on-hook voltage but will not allow on-hook messaging other than caller ID.

### CHANNEL BANK > MODULES > MENU > TANDEM

Set the port to use E&M signaling on the T-Span and either loop start or ground start supervision on the analog 2-wire interface. To access submenus for this item, use the arrow keys to scroll to the **TANDEM** column for the module you want to edit, and then press enter.

**CONVERSION MODE -** Sets the port to either **LOOP START** or **GROUND START** Mode. Default is **LOOP START.**

**SUPERVISION -** Sets the supervision method used to either **IMMEDIATE** or **WINK.** Default is **IMMEDIATE.**

**DIAL TONE -** Used to enable or disable the on-board dial tone generation. Dial Tone is supplied for 5 sec. Then it drops. It cannot be broken when dialing digits. Default is **DISABLE.**

**RING BACK TONE -** Used to enable or disable the option of generating ring back tone towards the T-span. Default is **DISABLE.**

**ANSWER SUPERVISION** - Causes the polarity of tip and ring to be reversed when the far-end answers. Can be enabled or disable. Default is **DISABLE.**

**DNIS OPTIONS** - Choices are **DISABLE, ENABLE,** and **ENABLE W/ NO ANSWER WINK.** Default is **DISABLE.**

**DNIS DELAY -** Sets the amount of time the voice module waits after it receives a wink before sending answer supervision if the **DNIS OPTION** is set to **ENABLE**. Choices are **0.5 SEC, 1.0 SEC, 1.5 SEC, 2.0 SEC, 2.5 SEC, 3.0 SEC,** and **5.0 SEC.** Default is **3.0 SEC.**

**FWD DISC DELAY -** In Tandem mode, defines the delay between the time the forward disconnect is received and the actual battery removal/reversal. Choices are **250 MSEC, 500 MSEC, 750 MSEC, 1 SEC,** and **2 SEC**. Default is **1 SEC**.

**FWD DISC BATTERY -** In Tandem mode, selects whether battery is to be removed or reversed during forward disconnect. Choices are **REMOVE** and **REVERSE.** Default is **REMOVE**.

## CHANNEL BANK > MODULES > ALARM (N/A)

## CHANNEL BANK > MODULES > ALARM HISTORY (N/A)

### CHANNEL BANK > MODULES > TEST > TEST

Choices are given below. Default is **NONE.**

**NONE -** Indicates that no test is currently active.

**DIGITAL NET LPBK -** Used to loop back DS0 data coming from the network for each channel. Received data is latched in on the appropriate receive time slot on the receive bus. This data is then placed on the transmit bus in the unit's transmit time slot.

**NETWORK ON-HOOK TEST -** Used to test signaling sent to the network by the unit. On-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

**NETWORK OFF-HOOK TEST -** Used to test signaling sent to the network by the unit. Off-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

**1 KHZ TONE-NEAR END -** This test option is only applicable for FXO and FXS modules. For Near End, the 2-wire side sends out a 1 kHz tone to verify talk path. (In the BCU, this tone option is bi-directional and can be heard at the Near End as well as the Far End.)

**1 KHZ TONE-FAR END -** This test option is only applicable for FXO and FXS modules. For Fear End, the tone side is sent out across the Network and can be heard if monitoring on the T1 as well as off of the Far End 2-wire side. Again, this verifies talk path. (In the BCU, this tone option is bi-directional and can be heard at the Near End as well as the Far End.)

**CUSTOMER RING TEST -** The customer ring test will activate the unit's ring relay in a 2-on /4-off cadence, providing ringing to the customer loop.

### CHANNEL BANK > MODULES > TEST > TEST STATUS

This option indicates whether a test is in progress.

### CHANNEL BANK > MODULES > STATUS > TA SIG

This parameter displays the status of the Transmit A signal bit. The high/low status is indicated by a 0 or 1.

### CHANNEL BANK > MODULES > STATUS > TB SIG

This parameter displays the status of the Transmit B signal bit. The high/low status is indicated by a 0 or 1.

### CHANNEL BANK > MODULES > STATUS > RA SIG

This parameter displays the status of the Receive A signal bit. The high/low status is indicated by a 0 or 1.

### CHANNEL BANK > MODULES > STATUS > RB SIG

This parameter displays the status of the Receive B signal bit. The high/low status is indicated by a 0 or 1.

# SECTION 4.1 T1 TDM RCU USER INTERFACE GUIDE

Provides detailed descriptions of all menu options and configuration parameters available for the Total Access 850.

This section of ADTRAN’s Total Access 850 System Manual is designed for use by network administrators and others who will configure and provision the system. It contains information about navigating the VT100 user interface, configuration information, and menu descriptions. This section provides details unique to the T1 TDM IADs. It contains an overview, application details, configuration information, and menu descriptions. It is recommended that you review Section 4.0, Commons User Interface Guide in addition to this section.

## CONTENTS

## FIGURES

## TABLES

## 1. T1 TDM RCU MODULE OVERVIEW

The Total Access T1 TDM RCU is one of several controller units for the Total Access 850 integrated access system. The RCU includes a T1 network interface DSX-1 (FT1) interface, Nx56/64 V.35 interface, and onboard IP router. Access to the RCU may be via the DB-9 craft port on the front of the card, the RJ-45 craft port on the read of the chassis, or telnet (from the LAN or WAN side). The RCU can provision, test, and provide status for any card in the IAD.

## 2. T1 TDM APPLICATION

The most common Total Access 8520 T1 TDM application include simultaneous support for the following:

- PBX connection via a DSX-1 interface
- Router connection via a V.35 interface
- LAN connection via a 10BaseT interface
- Up to 24 POTS connections via FXS interfaces (6 Quad FXS modules)

The Total Access 850 connects to the PSTN and Internet via a Class 5 switch (usually a Lucent 5ESS or Nortel DMS 500) and an ADTRAN Total Access 4303. This application is shown in Figure1.

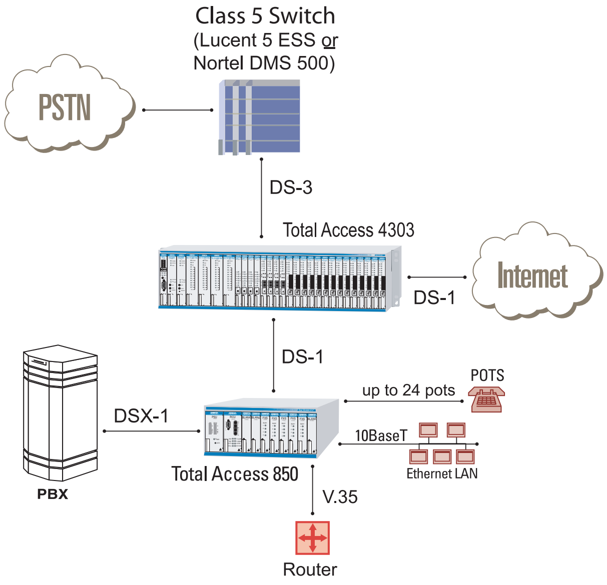


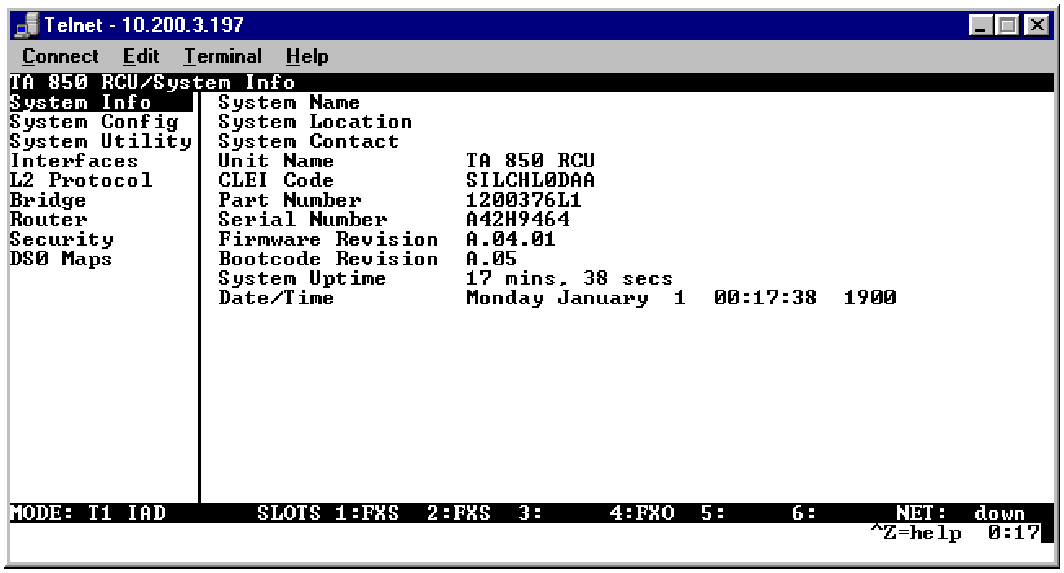
**Figure 1. Typical Total Access 850 T1 TDM Application**

## 3. CONFIGURATION

### SYSTEM INFO

The **SYSTEM INFO** menu provides basic information about the unit as well as data fields for editing information. Figure 2. displays the submenus that are available when you select this menu item.

> NOTE
>
> *All figures in this section will be representative of the Total Access 850 unit. Firmware revision will reflect A.04.01 for released revisions of software.*



```
TA 850 RCU/System Info
System Info     System Name
System Config   System Location
System Utility  System Contact
Interfaces      Unit Name          TA 850 RCU
L2 Protocol     CLEI Code          SILCHL0DAA
Bridge          Part Number        1200376L1
Router          Serial Number      A42H9464
Security        Firmware Revision  A.04.01
DS0 Maps        Bootcode Revision  A.05
                System Uptime      17 mins, 38 secs
                Date/Time          Monday January  1  00:17:38  1900

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET:  down
                                                                 ^Z=help  0:17
```

**Figure 2. System Info Menu**

### SYSTEM INFO > SYSTEM NAME

Provides a user-configurable text string for the name of the unit. This name can help you distinguish between different installations. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an underscore). This name will appear on the top line of all screens. The factory default is to have no entry in the system name field.

### SYSTEM INFO > SYSTEM LOCATION

Provides a user-configurable text string for the location of the unit. This field is to help you keep track of the actual physical location of the unit. You can enter up to 31 alphanumeric characters in this field, including spaces and special characters (such as an underscore). The factory default is to have no entry in the system location field.

### SYSTEM INFO > SYSTEM CONTACT

Provides a user-configurable text string for a contact name. You can use this field to enter the name, phone number, or E-mail address of a person responsible for the unit. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an underscore). The factory default is to have no entry in the system contact field.

### SYSTEM INFO > UNIT NAME

Product-specific name for the unit.

### SYSTEM INFO > CLEI CODE

The CLEI code for the unit.

### SYSTEM INFO > PART NUMBER

ADTRAN part number for the unit.

### SYSTEM INFO > SERIAL NUMBER

The serial number field will reflect serial number located on bottom of the unit's chassis.

### SYSTEM INFO > FIRMWARE REVISION

Displays the current firmware revision level of the unit.

### SYSTEM INFO > BOOTCODE REVISION

Displays the bootcode revision.

### SYSTEM INFO > SYSTEM UPTIME

Displays the length of time since the last reboot of the unit.

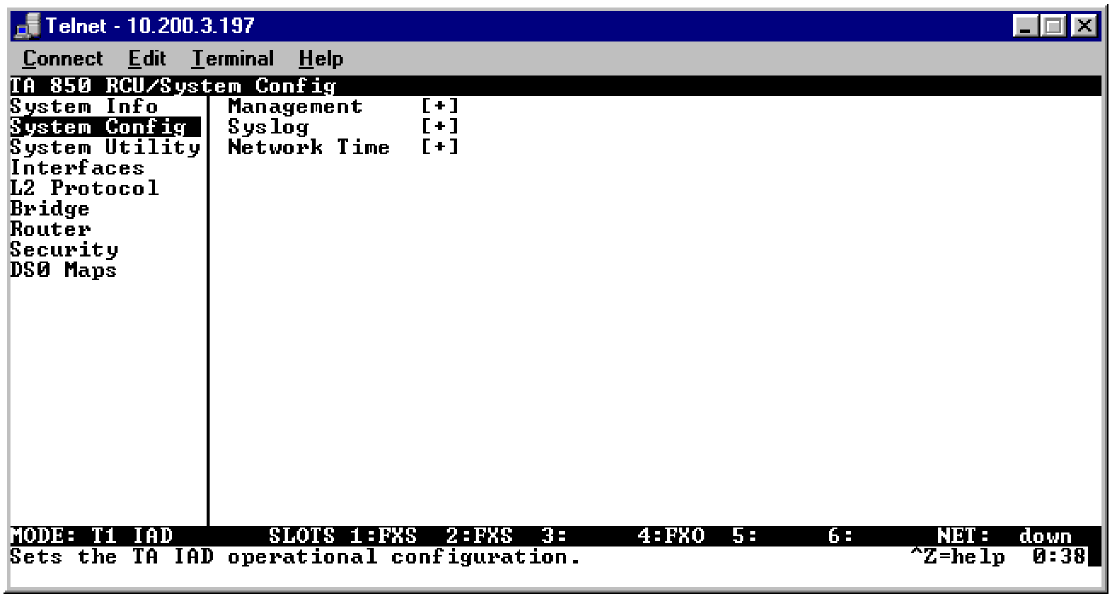
NOTE *Each time you reset the system, this value resets to 0 days, 0 hours, 0 min. and 0 secs.*

### SYSTEM INFO > DATE/TIME

Displays the current date and time, including seconds. This field can be edited. Enter the time in 24-hour format (such as 23:00:00 for 11:00 pm). Enter the date in mm-dd-yyyy format (for example, 10-30-1998).

### SYSTEM CONFIG

Set up the unit's operational configuration from the **SYSTEM CONFIG** menu. Figure 3. shows the items included in this menu.



```
TA 850 RCU/System Config
System Info    Management     [+]
System Config  Syslog         [+]
System Utility Network Time   [+]
Interfaces
L2 Protocol
Bridge
Router
Security
DS0 Maps

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:     4:FXO  5:      6:        NET:  down
Sets the TA IAD operational configuration.                          ^Z=help  0:38
```

**Figure 3. System Config Menu**

### System Config > Management

Set up the **CRAFT Port**, **Telnet Access**, **SNMP Management**, and **FDL Management** from this menu.

### System Config > Management > CRAFT Port

Set up the **CRAFT Port** parameters from this menu.

### System Config > Management > CRAFT Port > Password Protect

The unit's VT100 **CRAFT** port can be accessed via an RJ 48 connector located on the rear of the unit, or the DB9 connector on the front of the unit.

When **Password Protect** is set to **No**, the **CRAFT** port is not password protected. When **Yes** (def), the unit will prompt for a password upon startup.

### System Config > Management > CRAFT Port > Password

This is the text string that is used for comparison when password protecting the **CRAFT** port. By default, no password is entered. You can enter up to 30 characters in this field. Table 1 provides instructions for changing the password.

NOTE *The security level for the* **CRAFT** *port is always set to* **Full**. *This gives full access to all menus.*

NOTE *Passwords are case-sensitive and can contain up to 30 alphanumeric characters (including spaces and special characters).*

**Table 1. Instructions for Changing Passwords**

| Step | Action |
|---|---|
| **1** | Select the **PASSWORD** field—a new **PASSWORD** field displays. |
| **2** | Type the new password in the **ENTER** field. |
| **3** | Type the new password again in the **CONFIRM** field. |

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT >IDLE TIME

This option defines the amount of time in minutes user may stay connected without any activity on the **CRAFT PORT** before the user is automatically logged out of the system. A value of **0** disables this inactivity timer function enabling users to stay connected until manually logged out. The value range is **0** (def) to **255** (min).

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > BAUD RATE

This is the asynchronous rate that the **CRAFT** port will run. The possible values are **300, 1200, 2400, 4800, 9600, 19200, 38400**, **57600,** and **115200**. The default value is **9600**.

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > DATA BITS

This is the asynchronous bit rate that the **CRAFT** port will run. The possible values are **7** or **8** (def) bits.

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > PARITY

This is the asynchronous parity that the **CRAFT** port will run. The possible values are **NONE** (def), **ODD**, or **EVEN**.

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > STOP BITS

This is the number of stop bits used for the **CRAFT** port. The possible values are **1** (def), **1.5** or **2**.

### SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS

Activate the Telnet access and set up the various telnet parameters from this menu.

NOTE *The ATM D.01.XX firmware supports one telnet session active at a time. The TDM A.03.XX firmware supports one telnet session active at a time. The TDM A.04 firmware supports five simultaneous telnet sessions.*

### SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > ACCESS

Sets **ACCESS** to **ON** or **OFF.** The factory default value for this parameter is **ON**.

### SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > AUTHEN METHOD

Set up the telnet authentication method from this menu. The choices are **PASSWORD**, **RADIUS**, **PASSWORD/RADIUS**, and **RADIUS/PASSWORD**. **PASSWORD/RADIUS** indicates that the unit will try Password Authentication first and if that fails, it will try Radius Authentication. **RADIUS/PASSWORD** indicates that the unit will try Radius authentication first and if that fails, it will try Password authentication. The default is **PASSWORD**.

### SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > USER LIST

Add telnet users and control the telnet access conditions through this menu.

#### #

Display the index number of the telnet users. Up to four users can be configured for access to the unit. Each user can be assigned a security level and idle time.

#### NAME

The name is a text string of the user name for this session. You can enter up to 15 characters in this field. The factory default is no entry in the **NAME** field.

#### PASSWORD

When the authenticating method is password, or password radius, this text string is used for the password. You can enter up to 30 characters in this field. The factory default is no entry in this field.

#### IDLE TIME (MINS)

This sets the amount of time in minutes you can be idle before you are automatically logged off. The factory default is **10 MINUTES**. The range is 1-255 minutes.

#### LEVEL

This is the security level granted to the user. Table 2 gives a brief description of each level. The factory default is **FULL**.

**Table 2. Telnet Security Levels**

| **Security Level** | **Description** |
|---|---|
| Full | The user has all access to view and configure all menus (same as logging in to the **CRAFT** port) |
| Support | The user has read only access to view the **SYSTEM INFO** menu. The user has privileges to view and change everything under the **SYSTEM CONFIG** menu except for the **CRAFT** port settings, telnet access lists, and the SNMP management communities. The user has full access to the **SYSTEM UTILITY** menu, including the ability to upgrade firmware and reset the unit. The user has full access to the **INTERFACES, L2 PROTOCOL, BRIDGE, ROUTER,** and **DS0** menus. The user does not have the ability to set **RADIUS SERVER** settings under the **SECURITY** menu. |
| Config | The same privileges as support, except that the user does not have privileges to download firmware or configuration from the **SYSTEM UTILITY** menu. The user additionally does not have the privilege to reset the unit remotely, or enter the terminal menu. |
| Router | The user has read only privileges for the **SYSTEM INFO** menu. There is no access to the **SYSTEM CONFIG** menu. The user has **PING** and **TRACEROUTE** access from the **SYSTEM UTILITY** menu. The user is limited to ethernet configuration and status from the **INTERFACES** menu. The user has full access to the **BRIDGE** and **ROUTER** menus. Access is limited to filters only from the **SECURITY** menu. |
| Voice | The user has read only privileges for the **SYSTEM INFO** menu. The user has access to the **PING** and **TRACEROUTE** utilities from the **SYSTEM UTILITIES** menu. The user has full access to the FXS module from the **INTERFACES** menu. |
| Status | The user has read access of all menus except for the following: **SYSTEM CONFIG/CRAFT PORT, SYSTEM CONFIG/TELNET ACCESS, SYSTEM CONFIG/SNMP MANAGEMENT,** and **SECURITY/ RADIUS SERVER**. The user does not have access to **UPGRADE FIRMWARE, UPGRADE CONFIG, PING,** or **TRACEROUTE** menus. The user cannot reset the unit or enter terminal mode. |

## SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > IP ACCESS LIST

Set up the list of allowed telnet managers.

### NETWORK ADDRESS AND MASK

Enter a network address and subnet mask from which telnet access to the unit is allowed. When a remote unit requests telnet access to the unit, if the access list is empty or the remote's IP address matches a list entry, remote access is granted. A subnet mask of 0.0.0.0 will allow any host telnet access, regardless of the network address. A network address of 0.0.0.0 with corresponding netmask 255.255.255.255 will not allow any host telnet access.

The factory default is **0.0.0.0.** for both parameters, which will allow all users telnet IP access.

## SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT

Active the SNMP management and configure the SNMP communities and traps from this menu.

## SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT > ACCESS

When set to **OFF**, SNMP access is denied. When set to **ON**, the unit will respond to SNMP managers based on the configuration. The factory default is **ON**.

## SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT > COMMUNITIES

Set up the SNMP communities parameters from this menu.

### #

Displays the index number of the SNMP Communities.
This list is used to set up to 8 SNMP communities that the unit will allow

### NAME

This is the text string used to identify the SNMP community. The factory default is no entry in the name parameter.

### PRIVILEGE

The access for this manager can be assigned three levels. The factory default is **NONE**.

| | |
|---|---|
| **NONE** | No access is allowed for this community or manager. |
| **GET** | Manager can only read items. |
| **GET/SET** | Manager can read and set items. |

#### MANAGER IP

This may be used in conjunction with the Netmask field to define a range of manager IPs. A netmask of 255.255.255.255 defines a single IP as the manager host IP. The default value is **0.0.0.0**.

#### NETMASK

The mask is used to determine which bits of the **MANAGER IP** are significant. A "0" bit means "don't care." A "1" bit means that the corresponding address bits in the incoming SNMP packet must match the address bit in the defined **MANAGER IP**. The netmask of 255.255.255.255 defines a single IP as the manager host IP. The default value is **0.0.0.0**.

### SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT > TRAPS

Sets up the trap manager name and IP from this menu.

#### #

Displays the index number in the SNMP traps table.
This list allows up to 20 managers to be listed to receive traps.

**MANAGER NAME** is the text string describing the name of the entry. It is intended for easy reference and has no bearing on the SNMP trap function. You can enter up to 31 characters in this field. The factory default is no entry in the manager name field.

#### MANAGER IP

This is the IP address of the manager that is to receive the traps. The factory default is **0.0.0.0**.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT

Enables the FDL management and configures mode and IP addresses from this menu.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > MODE

This enables the FDL (only in ESF mode) to be used for management. Learning mode can also be enabled so the unit can "learn" its IP configuration to be used for its FDL management. Once it learns this information from, for example a Total Access 4303, the configuration items populate. The factory default is **ON**.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > LINK IP ADDRESS

This is the local IP address used for FDL management. The FDL uses a separate IP network for communication, distinct from the customer data that is configured under the **ROUTER** menus. The factory default is **0.0.0.0**.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > IP NETMASK

This is the subnet mask defining the IP network used for FDL management. The factory default is **0.0.0.0**.

### System Config > Management > FDL Management > Far-End IP Address

This is the far-end IP address used for the FDL management. The FDL is a separate IP network from the customer data that is configured under the **Router** menus. The factory default is **0.0.0.0**.

### System Config > Management > FDL Management > Learn Address

When set to **On**, the destination address on each received packet is assumed to be the FDL interface address. A 255.255.255.252 netmask is used, which determines the far-side address as well (since there can be only two addresses on a subnet with that netmask). When set to **Off,** the user must input the IP address assigned to the FDL interface. Default is **ON**.

### System Config > Management > FDL Management > Accept All SNMP

When set to **On**, SNMP gets/sets received over the FDL link are always accepted regardless of the community table. When set to **Off,** the community table is searched for valid manager IP addresses and the SNMP traffic is rejected if a match is not found. Default is **On**.

### System Config > Syslog

Configure the unit Syslog client for use with a Syslog server (supplied with ADTRAN Utilities or available on most Unix platforms) from this menu.

> NOTE *For additional information, reference RFC3164: The BSD Syslog Protocol.*

### System Config > Syslog > Syslog IP

IP address of the syslog daemon to which log message should be sent. The values must be dotted decimal notation.

### System Config > Syslog > Syslog Format

The **Syslog format** is the format of log messages. "**Adtran**" uses a format that is compatible with Adtran Utilities and forces the Syslog Facility to LOCAL0. **Unix** uses the traditional Unix format and reports at the configured facility level.

> NOTE *Adtran Utilities may malfunction if messages are received in the Unix format.*

### System Config > Syslog > Syslog Facility

The choices are: **Local0**, **Local1**, **Local2**, **Local3**, **Local4**, **Local5**, **Local6**, **Local7**. **Syslog Facility** is the facility level for all messages forwarded from the unit to the syslog server. This allows all messages received from the IAD to be filtered by facility level. See *RFC3164: The BSD Syslog Protocol*..

*This does not have to correspond to the facility level shown in the terminal mode option. See SYSLOG Facility using Terminal Mode on page 73.*

The remaining Syslog parameters have the following level choices:

FATAL (Highest priority)
ALERT
CRITICAL
ERROR
WARNING
NOTICE
INFO
DEBUG (Lowest priority)

Every log message generated by the IAD has a reporting level priority. If the message priority is lower than the configured priority for the destination log, the message is not forwarded to the syslog daemon. See *RFC3164: The BSD Syslog Protocol*. The lower the log level, the more messages that will be generated. Setting reporting levels to DEBUG may negatively affect the performance of the IAD, including causing the IAD to reset.

*ADTRAN recommends using DEBUG for only short periods of time for debug purposes only.*

## SYSLOG using Terminal Mode

Another option for configuring syslog is using the terminal mode command **log dump <logname>**. The logname must be all CAPS and be one of the following names:

FATAL
ALERT
CRITICAL
ERROR
WARNING
NOTICE
INFO
DEBUG

The command will dump all messages for the indicated log (**ALL LEVEL** shows all log messages) stored in the internal log buffer to the command line display.

### SYSTEM CONFIG > SYSLOG > ALL LEVEL

This entry allows setting the default reporting level for all log entries. If **ALL LEVEL** is a lower priority than the individual log entry level, **ALL LEVEL** overrides the individual log reporting level.

### SYSTEM CONFIG > SYSLOG > KERNEL LEVEL

Minimum required level for sending KERNEL log messages.

### SYSTEM CONFIG > SYSLOG > DHCP LEVEL

Minimum required level for sending DHCP log messages.

### SYSTEM CONFIG > SYSLOG > NTP LEVEL

Minimum required level for sending NTP log messages.

### SYSTEM CONFIG > SYSLOG > TFTP LEVEL

Minimum required level for sending TFTP log messages.

### SYSTEM CONFIG > SYSLOG > TELNET LEVEL

Minimum required level for sending TELNET log messages.

### SYSTEM CONFIG > SYSLOG > IP LEVEL

Minimum required level for sending IP log messages.

### SYSTEM CONFIG > SYSLOG > PPP LEVEL

Minimum required level for sending PPP log messages.

### SYSTEM CONFIG > SYSLOG > NAT LEVEL

Minimum required level for sending NAT log messages.

### SYSTEM CONFIG > SYSLOG > ARP LEVEL

Minimum required level for sending ARP log messages.

### SYSTEM CONFIG > SYSLOG > UDP LEVEL

Minimum required level for sending UDP log messages.

### SYSTEM CONFIG > SYSLOG > NETWRITE LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG > TCP LEVEL

Minimum required level for sending TCP log messages.

### SYSTEM CONFIG > SYSLOG > COMPSYS LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG > CONSOLE LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG > CFGXFER LEVEL

Minimum required level for sending configuration transfer log messages.

### SYSTEM CONFIG > SYSLOG > ROUTER LEVEL

Minimum required level for sending router log messages.

### SYSTEM CONFIG > SYSLOG > NONVOL LEVEL

Minimum required level for sending nonvolatile memory log messages.

### SYSTEM CONFIG > SYSLOG > NOKIA LEVEL

Minimum required level for sending log messages about communication with the Nokia DSLAM. Messages are only generated for products with an SDSL WAN interface.

### SYSTEM CONFIG > SYSLOG > AUTOBAUD LEVEL

Minimum required level for sending log messages about communication with the Lucent Stinger DSLAM. Messages are only generated for products with an SDSL WAN interface.

### SYSTEM CONFIG > SYSLOG > TOLLBRG LEVEL

Minimum required level for sending log messages about communication with the Tollbridge Voice Gateway. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > CMCP LEVEL

Minimum required level for sending log messages about communication with the CopperMountain DSLAM. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > SDSL LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG > L1 LEVEL

Minimum required level for sending log messages about WAN physical or Layer 1 connection.

### SYSTEM CONFIG > SYSLOG > ETH LEVEL

Minimum required level for sending log messages about Ethernet physical connection.

### SYSTEM CONFIG > SYSLOG > ICMP LEVEL

Minimum required level for sending ICMP log messages.

### SYSTEM CONFIG > SYSLOG > CONFIG LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG >DS0 LEVEL

Minimum required level for sending log messages about DSO mapping.

### SYSTEM CONFIG > SYSLOG > SELFTEST LEVEL

Minimum required level for sending log messages about selftest.

### SYSTEM CONFIG > SYSLOG > VOICE LEVEL

Minimum required level for sending log messages about AAL2 voices services.
Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > JETSTREAM LEVEL

Minimum required level for sending log messages about communication with the JetStream Voice Gateway. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > POTS LEVEL

Minimum required level for sending log messages about POTS line cards and services.

### SYSTEM CONFIG > SYSLOG > LESCAS LEVEL

Minimum required level for sending messages about communication with LESCAS compatible Voice Gateways. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > ATM LEVEL

Minimum required level for sending ATM log messages. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > COPPERCOM LEVEL

Minimum required level for sending log messages about communication with the CopperCom Voice Gateway. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > VOFR LEVEL

Minimum required level for sending voice-over-frame-relay log messages about communication with the CopperMountain DSLAM. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > XMODEM LEVEL

Minimum required level for sending XMODEM log messages for firmware and configuration transfers.

### SYSTEM CONFIG > SYSLOG > EMWEB LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG > FRELAY LEVEL

Minimum required level for sending frame relay log messages.

### SYSTEM CONFIG > SYSLOG > BRIDGE LEVEL

Minimum required level for sending bridge mode log messages.

### SYSTEM CONFIG > SYSLOG > MAINT LEVEL

Minimum required level for sending **CRAFT** port log messages.

### SYSTEM CONFIG > SYSLOG > HDLC LEVEL

Minimum required level for sending low level HDLC log messages.

### SYSTEM CONFIG > SYSLOG > VOATM LEVEL

Minimum required level for sending Voice-over-ATM log messages.

### SYSTEM CONFIG > SYSLOG > PPPOA LEVEL

Minimum required level for sending PPP-over-ATM log messages.

### SYSTEM CONFIG > SYSLOG > FDL LEVEL

Minimum required level for sending FDL log messages.

### SYSTEM CONFIG > NETWORK TIME

Activate the network time and configure the server type, time zone and various other network time parameters from this menu.

### SYSTEM CONFIG > NETWORK TIME > SERVER TYPE

The unit time can be entered manually from the **SYSTEM INFO** menu, or the unit can receive time from an NTP/SNTP server. The **NETWORK TIME** menu includes all parameters relating to how the unit communicates with the time server.

The server type defines the port on which the unit will listen to receive timing information from the time server. The choices are **NT TIME** and **SNTP**. When set to **NT TIME**, the unit will receive time from an NT server running SNTP software on its TIME port. When set to **SNTP**, the unit will receive time directly from an SNTP server. The factory default is **SNTP**.

### SYSTEM CONFIG > NETWORK TIME > ACTIVE

This network timing feature can be turned on and off. It determines whether the unit will request and receive time from a time server. The factory default is **NO**.

### SYSTEM CONFIG > NETWORK TIME > TIME ZONE

All time zones are based off of Greenwich Mean Time (GMT). The choices are listed below

•**GMT**<br>
•**GMT -5 (EASTERN)**<br>
•**GMT -6 (CENTRAL)**<br>
•**GMT -7 (MOUNTAIN)**<br>
•**GMT -8 (PACIFIC)**<br>
•**GMT -9 (ALASKA)**<br>
•**GMT -10 (HAWAII)**

The factory default is **GMT-6 (CENTRAL)**.

### SYSTEM CONFIG > NETWORK TIME > ADJUST FOR DAYLIGHT SAVING

Since some areas of the world use Daylight Savings Time, the unit is designed to adjust the time on the first Sunday in April and the last Sunday in October accordingly if this option is turned on. The factory default is **YES**.

### SYSTEM CONFIG > NETWORK TIME > HOST ADDRESS

This is the IP address of the time server that the unit will request and receive time from. The factory default is no entry in the host address field.

### SYSTEM CONFIG > NETWORK TIME > REFRESH

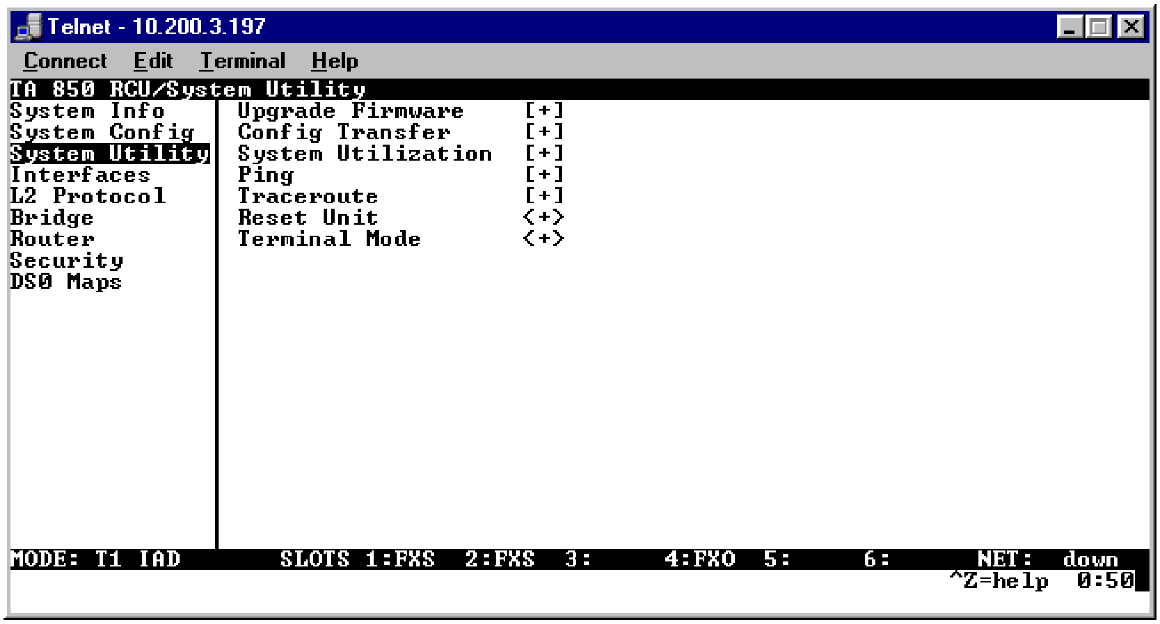
This is the interval of time between each request the unit sends out to the time server. A smaller refresh time guarantees that the unit receives the correct time from the server and corrects possible errors more quickly. This may be more taxing on the machine. A range of refresh times is available for the user to decide which is best for their unit. Choices include **5 MINS, 10 MINS, 15 MINS, 20 MINS, 25 MINS, 30 MINS, 35 MINS, 40 MINS, 45 MINS, 50 MINS, 55 MINS,** and **60 MINS**. The factory default is **60 MINS**.

### SYSTEM CONFIG > NETWORK TIME > STATUS

This displays the current status of the time negotiation process. If an error is displayed, check all connections and configurations to try to resolve the problem.

### SYSTEM UTILITY

Use the **SYSTEM UTILITY** menu to view and set the system parameters shown in Figure 4..



```
TA 850 RCU/System Utility
System Info     Upgrade Firmware    [+]
System Config   Config Transfer     [+]
System Utility  System Utilization  [+]
Interfaces      Ping                [+]
L2 Protocol     Traceroute          [+]
Bridge          Reset Unit          <+>
Router          Terminal Mode       <+>
Security
DS0 Maps

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:      4:FXO  5:      6:       NET:  down
                                                                ^Z=help  0:50
```

**Figure 4. System Utility Menu**

### System Utility > Upgrade Firmware

Select the firmware upgrade method and perform upgrade from this menu.

### System Utility > Upgrade Firmware > Transfer Method

The customer can update firmware when unit enhancements are released.

The two methods for upgrading are **XMODEM** and **TFTP**. (See the DLP section of this manual for more information.) **TFTP** requires a TFTP server running on the network. The unit starts a TFTP client function which gets the upgrade code from the TFTP server. Selecting **XMODEM** will load the upgrade code through the **CRAFT** port using any PC terminal emulator with XMODEM capability. The factory default is **TFTP**.

### System Utility > Upgrade Firmware > TFTP Server Address

This is required when the transfer method is TFTP. It is the IP address or domain name (if DNS is configured) of the TFTP server. The factory default is no entry in the **TFTP SERVER ADDRESS** field.

### System Utility > Upgrade Firmware > TFTP Server Filename

This is required when the transfer method is TFTP. It is the case-sensitive file name which contains the upgrade code. The factory default is no entry in the **TFTP Server Filename** field.

### System Utility > Upgrade Firmware > Transfer Status

This appears when TFTP is used. It displays the status of the transfer as it happens. Any error or success message will be displayed here.

### SYSTEM UTILITY > UPGRADE FIRMWARE > START TRANSFER

This activator is used when the configurable items in this menu are complete. This will initiate the transfer for either TFTP or XMODEM upgrades.

> NOTE *Before using* ***START TRANSFER****, the unit should have a valid IP address, subnet mask, and default gateway (if required). See DLP-002Setting IP Parameters for the Total Access 850 for more information.*

### SYSTEM UTILITY > UPGRADE FIRMWARE > ABORT TRANSFER

Use this activator to cancel any TFTP transfer in progress.

### SYSTEM UTILITY > CONFIG TRANSFER

Select the config transfer method and perform the transfer from this menu.

### SYSTEM UTILITY > CONFIG TRANSFER > TRANSFER METHOD

Sends a file containing the unit configuration to a PC connected to the **CRAFT** port using XMODEM protocol or to a file on a TFTP server using the TFTP protocol.

**CONFIG TRANSFER** also lets you save the unit configuration as a backup file, so you can use the same configuration with multiple units. In addition, **CONFIG TRANSFER** can retrieve a configuration file from a TFTP server.

To support these transfers, ADTRAN delivers a TFTP program with the unit called TFTP Server. You can configure any PC running Microsoft Windows with this software, and store a configuration file.

> NOTE *Before using* ***START TRANSFER****, the unit should have a valid IP address, subnet mask, and default gateway (if required). See DLP-002, Setting IP Parameters for the Total Access 850 for more information.*

Only one configuration transfer session (upload or download) can be active at a time. **XMODEM** and **TFTP** are supported.

### SYSTEM UTILITY > CONFIG TRANSFER > TFTP SERVER IP ADDRESS

Specifies the IP address of the TFTP server. Get this number from your system administrator. If using the ADTRAN Utilities TFTP server, this number appears in the TFTP server status window. The factory default value is **0.0.0.0**.

### SYSTEM UTILITY > CONFIG TRANSFER > TFTP SERVER FILENAME

Defines the name of the configuration file that you transfer to or retrieve from the TFTP server. The default name is **ta_iad.cfg**, but you can edit this name.

### SYSTEM UTILITY > CONFIG TRANSFER > CURRENT TRANSFER STATUS

Indicates the current status of the update.

### System Utility > Config Transfer > Previous Transfer Status

Indicates the status of the previous update.

### System Utility > Config Transfer > Load And Use Config

Retrieves the configuration file specified in the **TFTP Server Filename** field from the server. To start this command, enter **Y** to begin or enter **N** to cancel.

> CAUTION
>
> *If you execute this command, the unit retrieves the configuration file, reboots, then restarts using the new configuration.*

### System Utility > Config Transfer > Save Config Remotely

Saves the configuration file specified in **TFTP Server Filename** to the server identified in **TFTP Server IP Address**. To start this command, enter **Y** to begin or enter **N** to cancel.

> CAUTION
>
> *Before using this command, you must have identified a valid TFTP server in* **TFTP Server IP Address**.

### System Utility > System Utilization

View the CPU utilization stats from this menu.

### System Utility > System Utilization > Performance

Clear the system utilization stats and view the total and current CPU utilization stats from this menu.

### System Utility > System Utilization > Performance > Total Avg CPU Utilization

**Total Avg CPU Utilization** is a running total of CPU utilization since the last reset.

### System Utility > System Utilization > Performance > Current Avg CPU Utilization

**Current Avg CPU Utilization** is the running total of CPU utilization since the last clear.

### System Utility > System Utilization > Performance > Clear Stats

This activator will clear all the system utilization performance stats.

### System Utility > Ping

Activate the ping test and define the ping packet characteristics from this menu.

### SYSTEM UTILITY > PING > START/STOP

Activator to start and cancel a ping test.

NOTE *Only one ping session can be active at a time.*

NOTE *Diagnostic features such as ping, extended ping, traceroute, extended traceroute, and telnet client can also be performed via* ***TERMINAL MODE*** *(see page 83).*

### SYSTEM UTILITY > PING > HOST ADDRESS

IP address or domain name (if DNS is configured) of device to receive the ping. The factory default is no entry in the host address field.

### SYSTEM UTILITY > PING > SIZE (40-1500)

Total size of the ping to send. Range is **40** to **1500** bytes. The default is **64**.

### SYSTEM UTILITY > PING > # OF PACKETS

Total packets to send every 2 seconds. Setting this to **0** allows the client to ping continuously.
The default is **5**.

### SYSTEM UTILITY > PING > # TRANSMITS

Total packets sent (read only).

### SYSTEM UTILITY > PING > # RECEIVES

Total packets received (read only).

### SYSTEM UTILITY > PING > % LOSS

Percentage loss based on ping returned from host (read only).

### SYSTEM UTILITY > TRACEROUTE

Utility program used to trace a data path to a final destination.

### SYSTEM UTILITY > TRACEROUTE > TRACE TARGET

Specifies the IP address of the remote system to trace the routes to.

### SYSTEM UTILITY > TRACEROUTE > MAXIMUM HOPS

Specifies the maximum number of router exchanges allowed when traveling to the final destination (specified using the **TRACE TARGET** field) Range is **1** to **30**. Default is **30**.

### SYSTEM UTILITY > TRACEROUTE > TIMEOUT (IN SECS)

Specifies the maximum delay (in milliseconds) given to a host (along a path to the final destination) to respond to the probe datagram sent before considering the packet a failure.

### SYSTEM UTILITY > TRACEROUTE > RETRIES

Specifies the number of times the probe datagram is sent to each host (along the path to the final destination).

### SYSTEM UTILITY > TRACEROUTE > BEGIN TRACEROUTE

Activates the traceroute process by sending a probe datagram with a Time To Live (TTL) value of 1.

### SYSTEM UTILITY > RESET UNIT

Selecting this activator will power reset the unit.

### SYSTEM UTILITY > TERMINAL MODE

Selecting the terminal mode gives the user a command-line prompt to perform utilities such as pings, traceroutes, resets, firmware updates, configuration, and more. **TERMINAL MODE** can also be accessed by using the shortcut keys **CNTRL** T from other menu screens. From this command-line prompt, you can:

- Perform a reset with the command "reset"
- Perform a factory restore with the command "factory_reset"
- Configure the unit. The unit has the ability to download a text file which contains the configuration of the entire unit. This configuration may then be altered in a text editor, and then uploaded to a unit. (See DLP-013, *A.03 to A.04 Firmware Upgrade*, for further assistance.)
- Debug and troubleshoot. This function would be carried out with the assistance of ADTRAN Technical Support.
- Start and stop the fail-safe timer for the auto-config feature.
- Perform a firmware upgrade via TFTP.

  **upgrade_firmware *hostname filename***
- Use the **save** command to write the entire configuration to flash.
- Display the unit's MAC address with the command **mac**
- Perform a ping or extended ping. Syntax is:

  **ping hostname/address [repeat xx] [size xx] [timeout xx] [source xx] [noNat]**

  Options:

  | | |
  |---|---|
  | repeat <repeat count> | Number of pings to send (default 5) |
  | size (datagram size) | Range is 40-1500 |
  | timeout (seconds) | Timeout in seconds (range 1-10) |
  | source (address or name) | Source address or interface name to use |
  | noNat | Do not NAT the ping packet |

  Options may be entered in any order and may be truncated.
  Valid interface names are eth0, fdl0, ppp0, fr0, fr1, etc.

  Example usage: **ping 10.0.0.5 r si 1500 so eth0 n**

This will ping with a repeat count of 10. The datagram size is 1500 bytes, and the source address used in the ping packet will be the ethernet IP address. The “noNat” option has been specified, so if NAT is enabled, this packet will NOT be translated.

- Perform a traceroute or extended traceroute. Syntax is:

  **traceroute hostname/address [hops xx] [timeout xx] [retries xx] [source xx] [noNat]**

  Options:

| | |
|---|---|
| hops <hops count> | Max number of hops (default 30) |
| timeout <seconds> | Timeout in seconds (default 3) |
| retries <seconds> | Number of retries per hop (default 3) |
| source <address or name> | Source address or interface name to use |
| noNat | Do not NAT the trace packets |

  Options may be entered in any order and may be truncated.

  Valid interface names are eth0, fdl0, ppp0, fr0, fr1, etc.

  Example usage: **trace 10.0.0.5 h 20 t 1 r 1 so eth0**

  This will perform a trace to 10.0.0.5 with a max hop count of 20. The timeout for each hop is 1 second, and the retry count per hop is 1. The ethernet IP will be used as the source address, and the packet WILL go through NAT if NAT is enabled, meaning that the packet will be translated and the source address will be replaced by the NAPT address.

- Use the telnet client feature to telnet to a remote host. Syntax is:

  **telnet hostname/address [port xx]**

  Default port is 23 (TELNET).

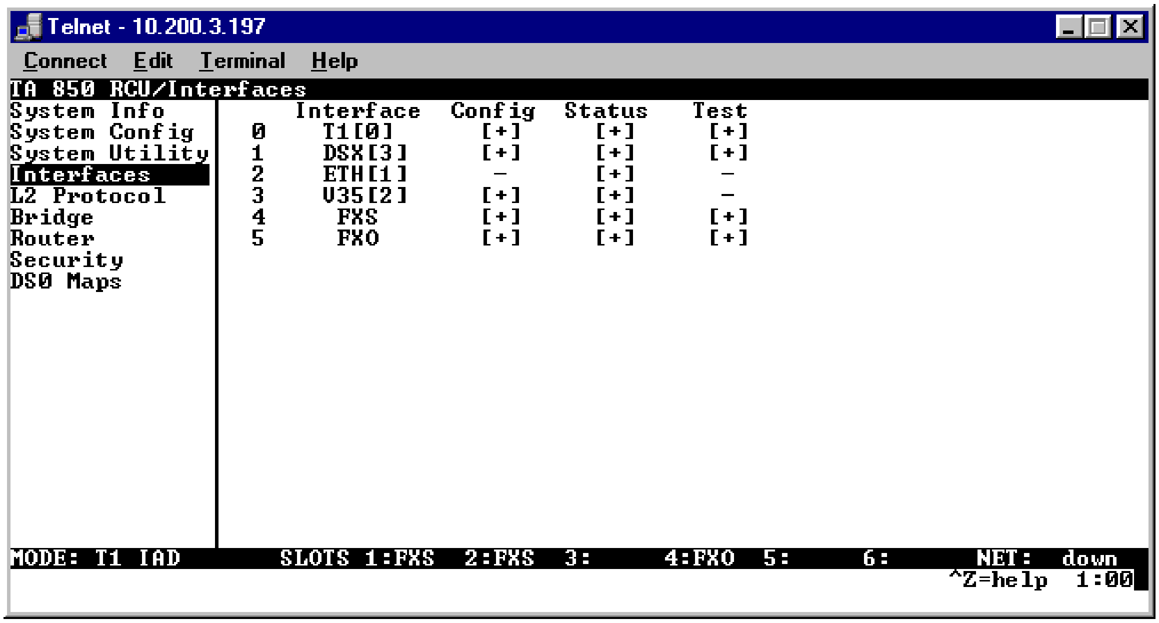
- To exit terminal mode, type **exit** or **!exit**,

  **exit -** if any configuration have been made, you will be prompted whether or not to save these changes. If no changes were made then the terminal session will exit without the confirm message.
  **!exit -** exit without saving or applying any configuration changes.

> NOTE *Extended ping, extended traceroute, and telnet client are new features initially available in A.04.02. These functions may be performed simultaneously from multiple user sessions.*

### INTERFACES

Use the **INTERFACES** menu to view and configure parameters for the **T1**, **ETHERNET**, **V.35**, and **FXS** interfaces as shown in Figure 5.



```
TA 850 RCU/Interfaces
System Info          Interface  Config  Status   Test
System Config    0     T1[0]      [+]     [+]     [+]
System Utility   1     DSX[3]     [+]     [+]     [+]
Interfaces       2     ETH[1]      -      [+]      -
L2 Protocol      3     V35[2]     [+]     [+]      -
Bridge           4      FXS       [+]     [+]     [+]
Router           5      FXO       [+]     [+]     [+]
Security
DS0 Maps




MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:       NET:  down
                                                                 ^Z=help  1:00
```

**Figure 5. Interfaces Menus**

### INTERFACES (T1[0])

View the T1 interface status and configure T1 parameters from this menu.

*The 0 in T1[0] represents a physical port. The T1 physical port is always 0.*

### INTERFACES (T1[0]) > CONFIG

Configure the various T1 parameters and enable/disable loopbacks from this menu.

### INTERFACES (T1[0]) > CONFIG > TIMING MODE

Choices are **NETWORK** and **INTERNAL**. Select **NETWORK** when the unit will receive timing from the network. Select **INTERNAL** when the unit will generate the timing. Default is **NETWORK**.

### INTERFACES (T1[0]) > CONFIG > FORMAT

This sets the frame format for the T1 interface. The setting must match the frame format of the circuit to which the interface is connected. Choices are **ESF** or **SF**. Extended Superframe (**ESF**) provides a non-disruptive means of full-time monitoring on the facility datalink (FDL). Default is **ESF**.

> NOTE *SF is equivalent to the D4 frame format.*

### INTERFACES (T1[0]) > CONFIG > LINE CODE

This sets the line code for the T1 interface. The setting must match the line code of the circuit to which the interface is connected. Choices are **B8ZS** (bipolar with 8-zero substitution) and **AMI** (alternate mark inversion). Default is **B8ZS**.

### INTERFACES (T1[0]) > CONFIG > EQUALIZATION

Select the line build out for the T1 interface. These are attenuation settings. 0 dB is the strongest signal and the other settings make the T1 transmit signal weaker. The setting of this field depends on whether the circuit is provisioned for DS1 by the telephone company. The choices are **0 dB**, **-7.5 dB**, **-15 dB**, **-22 dB**. Default is **0 dB**.

### INTERFACES (T1[0]) > CONFIG > CSU LPBK

Choices are **ENABLE**, **DISABLE**, and **DISABLE ALL**. Default is **ENABLE**. This allows the unit to either respond or not respond to CSU loop up commands.

### INTERFACES (T1[0]) > STATUS

Displays the T1 status including performance data and alarm histories.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE

Displays the T1 performance data.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > TIME FRAME

Choices are **CURRENT**, **15 MIN**, and **24 HR**. Default is **CURRENT**. The performance fields -- either **CURRENT**, **15 MIN**, or **24 HR**. -- provide status on key performance measures as specified in ANSI T1.403 and AT&T TR 54016 for each of the T1 ports. When **CURRENT** is chosen, the performance data for the current 15 minute window is shown.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > CLEAR

Clears information for the selected port. Press **<ENTER>** when the cursor is over this field to clear the data.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > ES

**ES** (Errored Second) - For ESF mode, an errored second is defined as a second with one or more Path Code Violations (PCVs), or one or more Out of Frame (OOF) defects, or one or more Controlled Slip events, or a detected AIS (blue alarm) defect. For D4 (SF) mode, the presence of Bipolar Violations (BPVs) also triggers an errored second.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > SES

**SES** (Severely Errored Second) - For ESF mode, an **SES** is a second with 320 or more PCVs, or one or more OOF defects, or a detected AIS defect. For D4 (SF) mode, an **SES** is a second with one or more Framing Error events, or an OOF defect, or at least 1544 Line Code Violations or more.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > SEF

**SEF** (Severely Errored Frame) - An **SEF** condition occurs when 2 out of 6 consecutive frame bits are in error.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > FS

**FS** (Frame Slip) - A frame slip is defined as one or more frame bit errors in a one-second interval.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > LCV

**LCV** (Line Code Violation) - A Line Code Violation is defined as a Bipolar Violation (BPV), not including the B8ZS code word if B8ZS is employed. The number displayed is **LCV** events, which is defined as one or more BPVs in a one-second interval.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > SLP

SLP (Slip Error Event) - This occurs when a received frame is either repeated or deleted. A **SLP** error indicates a timing problem.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > UAS

**UAS** (Unavailable Seconds) - When 10 consecutive **SES**s have been logged, the unit is declared in an unavailable state, the 10 **SES**s are cleared, and the Unavailable Seconds count begins to increment starting with 10. The unavailable state is cleared when 10 consecutive non-SES seconds have occurred.

### INTERFACES (T1[0]) > STATUS > ALARMS

Displays current alarms and alarm history for T1 interface.

### INTERFACES (T1[0]) > STATUS > ALARMS > CURRENT ALARMS

Displays the current alarms on the T1 interface. An asterisk in a field indicates that an alarm is active.

| | |
|---|---|
| LOS | Loss of Signal. No signal detected on port interface. |
| RED | Not able to frame data received on the port.<br>Alternately referred to as Out of Frame (OOF). |
| YELLOW | Remote alarm indicator (RAI) being received on port. |
| BLUE | Receiving unframed all ones from the port alarm indicator signal (AIS). |

### INTERFACES (T1[0]) > STATUS > ALARMS > ALARM HISTORY

Displays the alarm history for the T1 interface. An asterisk in a field indicates that an alarm has occurred on the T1 interface since the last clear history.

| | |
|---|---|
| LOS | Loss of Signal. No signal detected on port interface. |
| RED | Not able to frame data received on the port.<br>Alternately referred to as Out of Frame (OOF). |
| YELLOW | Remote alarm indicator (RAI) being received on port. |
| BLUE | Receiving unframed all ones from the port alarm indicator signal (AIS). |

### INTERFACES (T1[0]) > STATUS > ALARMS > CLEAR HISTORY

Selecting this activator will clear the Alarm History for the T1 interface.

### INTERFACES (T1[0]) > TEST

These options are used to initiate local and remote loopback tests and display the test status.

### INTERFACES (T1[0]) > TEST > LOC LB

Loopback of the local unit. Choices are **NONE**, **LINE**, **AND PAYLOAD**. **LINE** Loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **PAYLOAD** Loopback  is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

### INTERFACES (T1[0]) > TEST > REM LB

Loopback of remote unit. Choices are **NONE**, **LINE**, and **PAYLOAD**.  **LINE** Loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **PAYLOAD** Loopback is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

### INTERFACES (T1[0]) > TEST > TEST STATUS

Indicates whether a test is in progress.

### INTERFACES (DSX[3])

View the DSX1 interface status and configure T1 parameters from this menu.

NOTE *The 3 in DSX[3] represents a physical port. The DSX1 physical port is always 3.*

### INTERFACES (DSX[3]) > CONFIG

Configure the various DSX1 parameters and enable/disable loopbacks from this menu.

### INTERFACES (DSX[3]) > CONFIG > FORMAT

This sets the frame format for the DSX1 interface. The setting must match the frame format of the circuit to which the interface is connected. Choices are **ESF**, **SF**. Extended Superframe (**ESF**) provides a non-disruptive means of full-time monitoring on the facility datalink (FDL). Default is **ESF**.

NOTE *SF is equivalent to the D4 frame format.*

### INTERFACES (DSX[3]) > CONFIG > LINE CODE

This sets the line code for the DSX1 interface. The setting must match the line code of the circuit to which the interface is connected. Choices are **B8ZS** (bipolar with 8-zero substitution) and **AMI** (alternate mark inversion). Default is **B8ZS**.

### INTERFACES (DSX[3]) > CONFIG > EQUALIZATION

Select the line build out for the DSX1 interface. The choices are **0 dB**, **266** ft**,** **399** ft**,** **533** ft**,** **655** ft**,** or **-7.5 dB**. Default is **0 dB**. The 7.5 **dB** setting is provided for terminal equipment that has trouble recovering a full 0dB level signal (typically one with a DS1 long haul line interface).

### INTERFACES (DSX[3]) > CONFIG > CSU LPBK

Choices are **ENABLE**, **DISABLE**, and **DISABLE ALL**. Default is **ENABLE**. This allows the unit to either respond or not respond to CSU loop up commands.

### INTERFACES (DSX[3]) > STATUS

Displays the T1 status including performance data and alarm histories.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE

Displays the T1 performance data.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > TIME FRAME

Choices are **CURRENT**, **15 MIN**, and **24 HR**. Default is **CURRENT**. The performance fields -- either **CURRENT**, **15 MIN**, or **24 HR**. -- provide status on key performance measures as specified in ANSI T1.403 and AT&T TR 54016 for each of the T1 ports. When **CURRENT** is chosen, the performance data for the current 15 minute window is shown.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > CLEAR

Clears information for the selected port. Press **<ENTER>** when the cursor is over this field to clear the data.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > ES

**ES** (Errored Second) - For ESF mode, an errored second is defined as a second with one or more Path Code Violations (PCVs), or one or more Out of Frame (OOF) defects, or one or more Controlled Slip events, or a detected AIS (blue alarm) defect. For D4 (SF) mode, the presence of Bipolar Violations (BPVs) also triggers an errored second.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > SES

**SES** (Severely Errored Second) - For ESF mode, an **SES** is a second with 320 or more PCVs, or one or more OOF defects, or a detected AIS defect. For D4 (SF) mode, an **SES** is a second with one or more Framing Error events, or an OOF defect, or at least 1544 Line Code Violations or more.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > SEF

**SEF** (Severely Errored Frame) - An **SEF** condition occurs when 2 out of 6 consecutive frame bits are in error.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > FS

**FS** (Frame Slip) - A frame slip is defined as one or more frame bit errors in a one-second interval.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > LCV

**LCV** (Line Code Violation) - A Line Code Violation is defined as a Bipolar Violation (BPV), not including the B8ZS code word if B8ZS is employed. The number displayed is **LCV** events, which is defined as one or more BPVs in a one-second interval.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > SLP

SLP (Slip Error Event) - This occurs when a received frame is either repeated or deleted. A **SLP** error indicates a timing problem.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > UAS

**UAS** (Unavailable Seconds) - When 10 consecutive **SES**s have been logged, the unit is declared in an unavailable state, the 10 **SES**s are cleared, and the Unavailable Seconds count begins to increment starting with 10. The unavailable state is cleared when 10 consecutive non-SES seconds have occurred.

### INTERFACES (DSX[3]) > STATUS > ALARMS

Displays current alarms and alarm history for T1 interface.

### INTERFACES (DSX[3]) > STATUS > ALARMS > CURRENT ALARMS

Displays the current alarms on the T1 interface. An asterisk in a field indicates that an alarm is active.

| | |
|---|---|
| LOS | Loss of Signal. No signal detected on port interface. |
| RED | Not able to frame data received on the port.<br>Alternately referred to as Out of Frame (OOF). |

| | |
|---|---|
| YELLOW | Remote alarm indicator (RAI) being received on port. |
| BLUE | Receiving unframed all ones from the port alarm indicator signal (AIS). |

### INTERFACES (DSX[3]) > STATUS > ALARMS > ALARM HISTORY

Displays the alarm history for the T1 interface. An asterisk in a field indicates that an alarm has occurred on the T1 interface since the last clear history.

| | |
|---|---|
| LOS | Loss of Signal. No signal detected on port interface. |
| RED | Not able to frame data received on the port.<br>Alternately referred to as Out of Frame (OOF). |
| YELLOW | Remote alarm indicator (RAI) being received on port. |
| BLUE | Receiving unframed all ones from the port alarm indicator signal (AIS). |

### INTERFACES (DSX[3]) > STATUS > ALARMS > CLEAR HISTORY

Selecting this activator will clear the Alarm History for the T1 interface.

### INTERFACES (DSX[3]) > TEST

These options are used to initiate local and remote loopback tests and display the test status.

### INTERFACES (DSX[3]) > TEST > LOC LB

Loopback of the local unit. Choices are **NONE**, **LINE**, **AND PAYLOAD**. **LINE** Loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **PAYLOAD** Loopback is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

### INTERFACES (DSX[3]) > TEST > REM LB

Loopback of remote unit. Choices are **NONE**, **LINE**, and **PAYLOAD**. **LINE** Loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **PAYLOAD** Loopback is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

### INTERFACES (DSX[3]) > TEST > TEST STATUS

Indicates whether a test is in progress.

### INTERFACES (ETH[1])

View the Ethernet interface status and configure the Ethernet parameters from this menu.

> NOTE *The 1 in ETH[1] represents a physical port. The Ethernet physical port is always 1.*

### INTERFACES (ETH[1]) > STATUS > MAC ADDRESS

This is a read-only field which displays the unique MAC address programmed at ADTRAN.

### INTERFACES (V35[2])

View the V.35 interface status and configure the V.35 parameters from this menu.

> NOTE *The 2 in V35[2] represents a physical port. The V.35 physical port is always 2.*

### INTERFACES (V35[2]) > CONFIG

Configure the DTE leads from this menu.

### INTERFACES (V35[2]) > CONFIG > CTS

Sets the control characteristic of the clear-to-send lead. Choices are **NORMAL** (follows RTS) or **FORCE ON.** Default is **NORMAL.**

### INTERFACES (V35[2]) > CONFIG > DCD

Sets the control characteristic of the carrier detect lead. Choices are **NORMAL** (follows valid signal on the network interface) or **FORCE ON.** Default is **NORMAL.**

### INTERFACES (V35[2]) > CONFIG > DSR

Sets the control characteristic of the data set ready lead. Choices are **NORMAL** (follows DTR) or **FORCE ON**. Default is **NORMAL.**

### INTERFACES (V35[2]) > STATUS

View the status of the DTE leads from this menu.

### INTERFACES (V35[2]) > STATUS > RTS

View the status of Request to Send (RTS) lead. Possibilities are **OFF** or **ON**. This is a read-only field.

### INTERFACES (V35[2]) > STATUS > DTR

View the status of the Data Terminal Read (DTR) lead. Possibilities are **OFF** and **ON**. This is a read only field.

### INTERFACES (FXS)

View the FXS interface status and configure the FXS parameters from this menu.

### INTERFACES (FXS) > CONFIG

Configure the FXS mode, line impedance and Tandem parameters from this menu.

### INTERFACES (FXS) > CONFIG > PORT

Indicates the port on which the FXS is installed.

### INTERFACES (FXS) > CONFIG > MODE

Choices are given below. Default is **LOOP START.**

NOTE *This mode needs to be set based on how the network is set up and how each port is being used. Each port does not need to be set to the same mode.*

**LOOP START** Sets the port to use FXS loop start signaling on the T-span and loop start supervision on the analog 2-wire interface.

**GROUND START** Sets the port to use FXS ground start signaling on the T-span and ground start supervision on the analog 2-wire interface.

**TR08 SINGLE** Sets the port to use Single Party Channel Unit signaling on the T-span (as defined by TR-TSY-000008) and loop start supervision on the analog 2-wire interface.

**TR08 UVG** Sets the port to us Universal Voice Grade signaling on the T-span (as defined by TR-TSY-000008) and either loop start or ground start supervision on the analog 2-wire interface.

**DPO** Sets the port to use Dial Pulse signaling to originate dialed numbers.

**TANDEM (E&M)** Sets the port to use E&M signaling on the T-span and either loop start or ground start supervision on the analog 2-wire interface. See the **TANDEM** submenus for more information.

### INTERFACES (FXS) > CONFIG > TX (dB)

Sets the TX direction level points. This signal will change the volume of the voice. TX (dB) is the signal that is transmitted out the T1, with 0 dB being the strongest. If the volume is too loud across the T1, this number should be increased. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **6.0 dB**.

### INTERFACES (FXS) > CONFIG > RX (dB)

Sets the RX direction level points. This signal will change the volume of the voice. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **3.0 dB**. The maximum signal is 0.0. dB.

### INTERFACES (FXS) > CONFIG > SVC MODE

Indicates whether the module is **IN SERVICE** or **OUT OF SVC**. This does not indicate whether the port has been mapped. For proper operation, the port must be mapped using the **DS0 MAPS** menu. Default is **IN SERVICE.**

### INTERFACES (FXS) > CONFIG > LINE Z

Sets the line impedance. Choices are **600 OHMS, 900 OHMS, 600 OHMS + 2.16µF, 900 OHMS + 2.16µF,** and **AUTO**. The line impedance of each port is based on the size of the network. Default is **600 OHMS**.

### INTERFACES (FXS) > CONFIG > MSG IND

This is better referred to as On-Hook Message Waiting. When this is set to **ENABLE,** talk path is always open, even in On-Hook conditions, in order for these FXS message tones to pass through. Default is **DISABLE**. Enabling on-hook message waiting will allow message lamp usage but will cause a lower on-hook voltage. Disabling this feature will allow higher on-hook voltage but will not allow on-hook messaging other than caller ID.

### INTERFACES (FXS) > CONFIG > TANDEM

Sets the port to use E&M signaling on the T-Span and either loop start or ground start supervision on the analog 2-wire interface. To access submenus for this item, use the arrow keys to scroll to the **TANDEM** column for the corresponding module, and then press **<ENTER>**.

### INTERFACES (FXS) > CONFIG > TANDEM > CONVERSION MODE

Sets the port to either **LOOP START** or **GROUND START** mode. Default is **LOOP START**.

### INTERFACES (FXS) > CONFIG > TANDEM > SUPERVISION

Sets the supervision method used to either **IMMEDIATE** or **WINK**. Default is **IMMEDIATE**.

### INTERFACES (FXS) > CONFIG > TANDEM > DIAL TONE

Used to enable or disable the on-board dial tone generation. Dial Tone is supplied for 5 sec; then it drops. It cannot be broken when dialing digits. Default is Dis**ABLE**.

### INTERFACES (FXS) > CONFIG > TANDEM > RING BACK TONE

Used to enable or disable the option of generating ring back tone towards the T-span. Default is **DISABLE**.

### INTERFACES (FXS) > CONFIG > TANDEM ANSWER SUPERVISION

Causes the polarity of tip and ring to be reversed when the far-end answers. Can be enabled or disabled. Default is D**ISABLE**.

### INTERFACES (FXS) > CONFIG > TANDEM > DNIS OPTIONS

This parameter is used in conjunction with D**NIS DELAY**. Choices are **DISABLE**, **ENABLE**, and **ENABLE W/ NO ANSWER WINK**. Default is **DISABLE**.

### INTERFACES (FXS) > CONFIG > TANDEM > DNIS DELAY

Sets the amount of time the voice module waits after it receives a wink before forwarding a DNIS digit if the D**NIS OPTION** is set to **ENABLE**. Choices are **0.5 SEC**, **1.0 SEC**, **2.0 SEC**, **2.5 SEC**, **3.0 SEC**, and **5.0 SEC**. Default is **3.0 SEC**.

### INTERFACES (FXS) > CONFIG > TANDEM > FWD DISC DELAY

In Tandem mode, **FWD DISC DELAY** defines the delay between the time the forward disconnect is received and the actual battery removal/reversal. Choices are **250 MSEC**, **500 MSEC**, **750 MSEC**, **1 SEC**, and **2 SEC**. Default is **1 SEC**.

### INTERFACES (FXS) > CONFIG > TANDEM > FWD DISC BATTERY

In Tandem mode, selects whether battery is to be removed or reversed during forward disconnect. Choices are **REMOVE** and **REVERSE**. Default is **REMOVE**.

### INTERFACES (FXS) > STATUS

Displays the status of the FXS signal bits.

### IINTERFACES (FXS) > STATUS > PORT

Displays the port number.

### INTERFACES (FXS) > STATUS > TA SIG

This parameter displays the status of the Transmit A signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXS) > STATUS > TB SIG

This parameter displays the status of the Transmit B signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXS) > STATUS > RA SIG

This parameter displays the status of the Receive A signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXS) > STATUS > RB SIG

This parameter displays the status of the Receive B signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXS) > TEST

Activate tests and monitor test status on a per port basis from this menu.

### INTERFACES (FXS) > TEST > PORT

Displays the port number.

### Interfaces (FXS) > Test > Test

Choices are given below. Default is **None**.

**None** Indicates that no test is currently active.

**Digital Network Lpbk** Used to loop back DS0 data coming from the network for each channel. Received data is latched in on the appropriate receive time slot on the receive bus. This data is then placed on the transmit bus in the unit’s transmit time slot.

**Network On Hook Test** Used to test signaling sent to the network by the unit. On-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

**Network Off Hook Test** Used to test signaling sent to the network by the unit. Off-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

**1 kHz Tone-Near End** For Near End, the 2-wire side sends out a 1 kHz tone to verify talk path.

**1 kHz Tone-Far End** For Far End, the tone side is sent out across the Network and can be heard if monitoring on the T1 as well as off of the Far End 2-wire side. This verifies talk path.

**Customer Ring Test** The customer ring test will activate the unit’s ring relay in a 2-on /4-off cadence, providing ringing to the customer loop.

### Interfaces (FXS) > Test > Test Status

This option indicates whether a test is in progress.

### Interfaces (FXO)

View the FXS interface status and configure the FXS parameters from this menu.

### Interfaces (FXO) > Config

Configure the FXS mode, line impedance, and Tandem parameters from this menu.

### Interfaces (FXO) > Config > Port

Indicates the port on which the FXS is installed.

### INTERFACES (FXO) > CONFIG > MODE

Choices are given below. Default is **LOOP START.**

> *This mode needs to be set based on how the network is set up and how each port is being used. Each port does not need to be set to the same mode.*

**LOOP START** Sets the port to use FXO loop start signaling on the T-span and loop start supervision on the analog 2-wire interface.

**GROUND START** Sets the port to use FXO ground start signaling on the T-span and ground start supervision on the analog 2-wire interface.

**DPO** Sets the port to use Dial Pulse signaling to originate dialed numbers.

### INTERFACES (FXO) > CONFIG > TX (dB)

Sets the TX direction level points. This signal will change the volume of the voice. TX (dB) is the signal that is transmitted out the T1, with 0 dB being the strongest. If the volume is too loud across the T1, this number should be increased. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **0.0 dB**.

### INTERFACES (FXO) > CONFIG > RX (dB)

Sets the RX direction level points. This signal will change the volume of the voice. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **0.0 dB**.

### INTERFACES (FXO) > CONFIG > SVC MODE

Indicates whether the module is **IN SERVICE** or **OUT OF SVC**. This does not indicate whether the port has been mapped. For proper operation, the port must be mapped using the **DS0 MAPS** menu. Default is **IN SERVICE.**

### INTERFACES (FXO) > STATUS

Displays the status of the FXO signal bits.

### INTERFACES (FXO) > STATUS > PORT

Displays the port number.

### INTERFACES (FXO) > STATUS > TA SIG

This parameter displays the status of the Transmit A signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXO) > STATUS > TB SIG

This parameter displays the status of the Transmit B signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXO) > STATUS > RA SIG

This parameter displays the status of the Receive A signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXO) > STATUS > RB SIG

This parameter displays the status of the Receive B signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXO) > TEST

Activate tests and monitor test status on a per port basis from this menu.

### INTERFACES (FXO) > TEST > PORT

Displays the port number.

### INTERFACES (FXO) > TEST > TEST

Choices are given below. Default is **NONE**.

**NONE** Indicates that no test is currently active.

**DIGITAL NETWORK LPBK** Used to loop back DS0 data coming from the network for each channel. Received data is latched in on the appropriate receive time slot on the receive bus. This data is then placed on the transmit bus in the unit's transmit time slot.

**NETWORK ON HOOK TEST** Used to test signaling sent to the network by the unit. On-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

**NETWORK OFF HOOK TEST** Used to test signaling sent to the network by the unit. Off-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

**1004 HZ - 0DCBM0 TONE GEN** Used to verify talk path by sending out 1004 Hz tone to test across the network. Monitoring of the T1 as well as the Far-End 2-wire side verifies the talk path if the tone is heard.

### INTERFACES (FXO) > TEST > TEST STATUS

This option indicates whether a test is in progress.

### INTERFACES (DSX CARD)

View the DXS Card interface status and configure the DXS Card  parameters from this menu.

### INTERFACES (DSX CARD) > CONFIG

Configures the DSX format and code from this menu.

### INTERFACE (DSX CARD) > CONFIG > SLOT

Indicates the slot in which the DSX is installed.

### INTERFACE (DSX CARD) > CONFIG > PORT

Indicates the port on which the DXS is installed.

### INTERFACE (DSX CARD) > CONFIG > FORMAT

This setting must match the frame format of the circuit to which the interface is connected. Choices are **ESF** and **SF**. Extended Superframe (ESF) provides a non-disruptive means of full-time monitoring on the facility data link (FDL). The default is **ESF**.

> NOTE
>
> ***SF*** *is equivalent to the D4 frame format.*

### INTERFACE (DSX CARD) > CONFIG > LINE CODE

This setting must match the line code of the circuit to which the interface is connected. Choices are **B8ZS** (bipolar with 8-zero substitution) and **AMI** (alternate mark inversion). The default is **B8ZS**.

### INTERFACES (DSX CARD) > STATUS > ALARMS > CURRENT ALARMS

Displays the current alarms on the T1 interface. An asterisk in a field indicates that an alarm is active.

| | |
|---|---|
| LOS | Loss of Signal. No signal detected on port interface. |
| RED | Not able to frame data received on the port.<br>Alternately referred to as Out of Frame (OOF). |
| YELLOW | Remote alarm indicator (RAI) being received on port. |
| BLUE | Receiving unframed all ones from the port alarm indicator signal (AIS). |

### INTERFACES (DSX CARD) > STATUS > ALARMS > ALARM HISTORY

Displays the alarm history for the T1 interface. An asterisk in a field indicates that an alarm has occurred on the T1 interface since the last clear history.

| | |
|---|---|
| LOS | Loss of Signal. No signal detected on port interface. |
| RED | Not able to frame data received on the port.<br>Alternately referred to as Out of Frame (OOF). |
| YELLOW | Remote alarm indicator (RAI) being received on port. |
| BLUE | Receiving unframed all ones from the port alarm indicator signal (AIS). |

### INTERFACES (DSX CARD) > STATUS > ALARMS > CLEAR HISTORY

Selecting this activator will clear the Alarm History for the T1 interface.

### INTERFACES (DSX CARD) > TEST

These options are used to initiate local and remote loopback tests and display the test status.

### INTERFACES (DSX CARD) > TEST > LOC LB

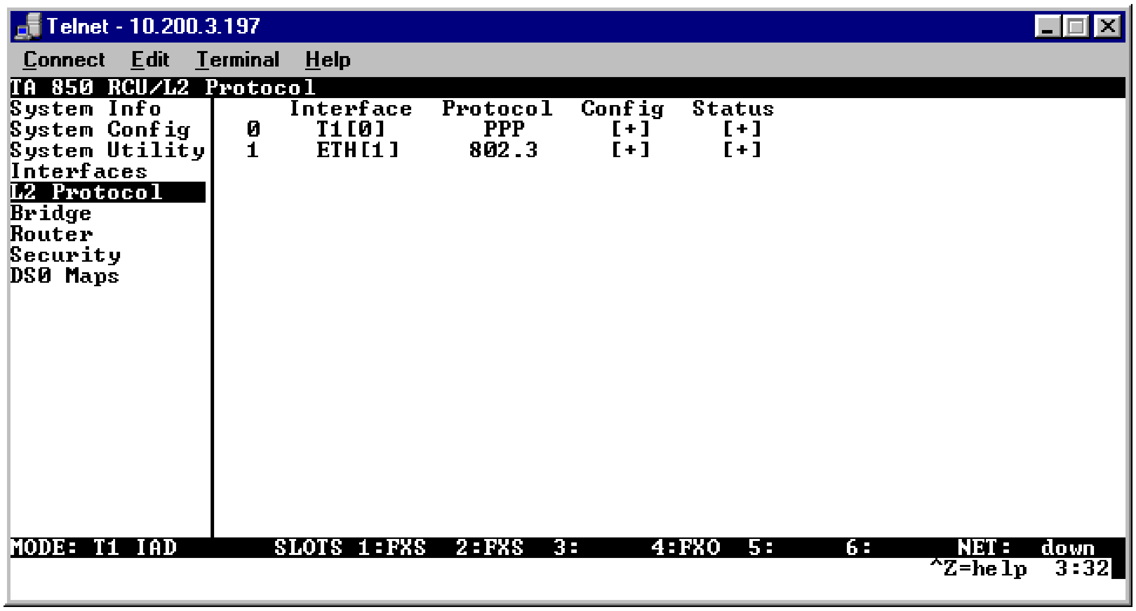
Loopback of the local unit. Choices are **NONE**, **LINE**, **AND PAYLOAD**. **LINE** Loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **PAYLOAD** Loopback  is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

### INTERFACES (DSX CARD) > TEST > TEST STATUS

Indicates whether a test is in progress.

### L2 PROTOCOL

Use the L2 protocol menu to select the L2 protocol, configure the protocol specific parameters and view the status as shown in Figure 6..



```
TA 850 RCU/L2 Protocol
System Info         Interface  Protocol  Config  Status
System Config   0    T1[0]      PPP       [+]     [+]
System Utility  1    ETH[1]     802.3     [+]     [+]
Interfaces
L2 Protocol
Bridge
Router
Security
DS0 Maps

MODE: T1 IAD      SLOTS 1:FXS  2:FXS  3:     4:FXO  5:      6:       NET:  down
                                                               ^Z=help  3:32
```

**Figure 6.  L2 Protocol Menu**

### L2 PROTOCOL (T1[0])

Configure the L2 Protocol parameters and view the status of the T1 interface using ATM protocol from this menu.

> NOTE *The 0 in T1[0] represents a physical port. The T1 physical port is always 0.*

### L2 PROTOCOL (T1[0]) > PROTOCOL

Configure the L2 protocol mode. Choices are PPP, FRE, and Auto. The default is Auto. Selecting Auto enable the Auto-config feature.

### L2 PROTOCOL (T1[0]) > PROTOCOL > PPP

Point-to-Point Protocol (PPP) is an 8-bit serial protocol which allows a PC to connect as a TCP/IP host to a network through an asynchronous port. PPP is used for connection from a PC to an Internet Service Provider (ISP) for Internet access. PPP works over synchronous and asynchronous circuits. Router-to-router and host-to-network connections can be made via PPP. PPP includes error detections which Serial Line Internet Protocol (SLIP) and other protocols do not.

### L2 PROTOCOL (T1[0]) > PROTOCOL > FRE

Frame Relay is a switched data link layer protocol that handles multiple virtual circuits using High-Level Data Link Control (HDLC) encapsulation. Frame Relay uses statistical multiplexing as opposed to time-division-multiplexing to multiplex many logical connections over a single physical link. It contains a cyclical redundancy check (CRC) for detecting bad data, but leaves the error correction algorithms to be performed by higher protocol layers. Similarly, Frame Relay uses simple congestion notification. This notification in turn can alert higher-layer protocols to exercise flow control. These characteristics allow Frame Relay to provide a more flexible and efficient use of bandwidth.

### L2 PROTOCOL (T1[0]) > PROTOCOL > AUTO

Setting the **L2 PROTOCOL** to A**UTO** allows the unit to automatically detect the **L2 PROTOCOL** from the network.

> NOTE *The **L2 PROTOCOL** must be set to **AUTO** in order to use the Auto-config feature.*

### L2 PROTOCOL (T1[0] - PPP)

Configure the **L2 PROTOCOL** parameters and view the status of the T1 interface using PPP protocol from this menu.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG

Configure the **L2 PROTOCOL** parameters for the T1 interface using PPP protocol.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > MODE

Select the **L2 PROTOCOL** mode. Choices are **ROUTE IP**, **BRIDGE ALL**, and Route IP/Bridge Other. The default is **ROUTE IP**.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > AUTHENTICATION

The Authentication menu contains the required parameters for the authentication of the PPP peer and for being authenticated by the PPP peer. Authentication is applied between the unit and the PPP peer as described in the Authentication submenus.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > AUTHENTICATION > TX METHOD

This parameter specifies how the unit is to be authenticated by the PPP peer. There are four possible selections. Default is **NONE**.

| | |
|---|---|
| **NONE** | The connection will not allow the PPP peer to authenticate it |
| **PAP, CHAP, OR EAP** | The unit will as for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** or **PAP**. |
| **CHAP OR EAP** | The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** but not **PAP**. |
| **EAP ONLY** | The unit will only allow EAP to be negotiated. If the PPP peer is not capable of doing EAP, then the connection will not succeed. |
| **PAP ONLY** | The unit will only allow **PAP** to be negotiated. If the PPP peer is not capable of doing **PAP**, then the connection will not succeed. |

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP

Configure the PPP specific parameters such as **MAX CONFIG**, **MAX TIMER**, **MAX FAILURE**, and **FORCE PEER IP ADDRESS** from this menu.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > MAX CONFIG

This value is the number of unanswered configuration-requests that should be transmitted before resetting PPP negotiations. The possible values are **5**, **10**, **15** and **20** (default).

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > MAX TIMER (SEC)

This value is the numbers of seconds to wait between unanswered configuration-requests. The possible values are **1 SEC**, **2 SECS**, **3 SECS (DEFAULT)**, **5 SECS** and **10 SECS**.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > MAX FAILURE

Due to the nature of PPP, configuration options may not be agreed upon between two PPP peers. This value is the number of configuration-naks that should occur before an option is configuration-rejected. The possible values are **5 (DEFAULT)**, **10**, **15**, and **20**.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > FORCE PEER IP ADDRESS

This option forces the PPP to negotiate the IP address entered instead of allowing the other an address to be assigned by the remote end.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > KEEPALIVE PERIOD

This option allow the user to generate PPP keepalive packets that can be sent one every 1 minute, 2 minutes or every 5 minutes. A value of 0 (def) disables the PPP keepalive packet generating feature.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > STATUS

View the **L2 PROTOCOL** status for the T1 interface using the PPP protocol.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > STATUS > LCP

Link Control Protocol. Reflects the LCP layer active.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > STATUS > BCP

Shows the UP if PPP Bridge Control Protocol has negotiated successfully.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > STATUS > IPCP

Shows UP if PPP IP Control Protocol has negotiated successfully.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > STATUS > UP TIME

Displays how long the PPP session has been connected.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > STATUS > TX PKTS

Number of packets transmitted.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > STATUS > TX BYTES

Number of bytes transmitted.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > STATUS > RX BYTES

Number of bytes received.

### L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > STATUS > CLEAR STATS

Selecting the activator will clear the PP stats.

### L2 PROTOCOL (T1[0] - FRE)

Configure the **L2 PROTOCOL** parameters and view the status of the T1 interface using Frame Relay protocol from this menu.

### L2 PROTOCOL (T1[0] - FRE) > CONFIG

Configure the L2 protocol parameters for the T1 interface using the Frame Relay protocol.

### L2 PROTOCOL (T1[0] - FRE) > CONFIG > MAINTENANCE PROTOCOL

The Frame Relay maintenance protocol is used on the WAN port. The maintenance protocol is used to send link status and virtual circuit information between Frame Relay switches and other devices (such as routers_ that communicate with them. Possible choices are as follows:

**ANNEX D (ANSI)** This ANSI standard ANSI T1.617-D and is the most commonly used in the United States.

**ANNEX A (Q933A)** This is the CCITT European standard, ITU-T Q.933-A.

**LMI** This was developed by a vendor consortium and is also known as the "Consortium" management interface specification. It is still used by some carriers in the United States.

**STATIC (NO SIG)** This should be selected when there is no Frame Relay switch in the circuit. The DLCIs are assigned in the DLCI Mapping and must be the same for the device it will communicate with.

The default value is **ANNEX D (ANSI)**.

### L2 PROTOCOL (T1[0] - FRE) > CONFIG > POLLING FREQUENCY (5-30)

This parameter is the interval that the unit polls the Frame Relay switch using the maintenance protocol selected. The unit is required to poll the Frame Relay switch periodically to determine whether the link is active. The value is in seconds and ranges from **5** to **30** seconds with a default of **10 SECONDS**.

### L2 PROTOCOL (T1[0] - FRE) > CONFIG > DLCI MAPPING

This menu allows each DLCI to be mapped to a particular Frame Relay maintenance protocol. Each protocol parameter can be individually configured for each DLCI. By factory default, the DLCI map is empty.

When empty and a maintenance protocol other than the static is used, the unit will poll the switch to determine which DLCIs are active. These active DLCIs will attempt to determine the IP addresses on the other end of the virtual circuit using Inverse ARP (IARP). If there is a response, the network learned will be added to the router tables and the virtual circuit will be treated as an unnumbered interface. Bridge connections are made using bridge group 1. When more than one DLCI mapping is listed, the unit will try to match the DLCIs learned from the Frame Relay switch with the DLCI values in the map. If there is a match, the protocols specified in the map are used. However, if an active DLCI is not in the list, the unit looks for an entry that has 0 in the DLCI field. The is entry is considered the default entry to use when no match occurs. If this default entry is not present, the unit falls back to using IARP to determine the protocols to use with that particular virtual circuit. If a static maintenance protocol is used, at least one DLCI mapping must be specified.

NOTE *To insert a new profile, press the **I** key when over the **Num** column. A new inserted profile will always be set up with the default parameters. To copy parameters from an old profile to this newly inserted profile, use the copy (**C**) and paste (**P**) keys. Entire configuration trees can be copied with this method.*

NOTE *To delete an unused profile, use the **D** key when the cursor is over the number in the **Num** column. Once deleted, the profile is gone permanently.*

### L2 PROTOCOL (T1[0] - FRE) > CONFIG > DLCI MAPPING > NUM

Displays the index number in the DLCI mapping table.

### L2 PROTOCOL (T1[0] - FRE) > CONFIG > DLCI MAPPING > ACTIVE

When this parameter is set to YES (def), the mapping is used to determine the protocols used. If set to **NO**, the unit will ignore the virtual circuit with this DLCI.

### L2 PROTOCOL (T1[0] - FRE) > CONFIG > DLCI MAPPING INTERFACE

Shows the user the physical and logical port associated with each DLCI. This is a read-only field.

### L2 PROTOCOL (T1[0] - FRE) > CONFIG > DLCI MAPPING > DLCI

This DLCI (Data Link Connection Identifier) number identifies the virtual circuit being configured.

### L2 PROTOCOL (T1[0] - FRE) > CONFIG > DLCI MAPPING > MODE

The mode identifies how the data will be forwarded. The choices are:

| | |
|---|---|
| **ROUTE IP** | All IP data for this DLCI will be routed. |
| **BRIDGE ALL** | All data for this DLCI will be bridged. |
| **ROUTE UIP/BRIDGE OTHER** | All IP data will be routed. All other data will be bridged. |

The default is **ROUTE IP**.

### L2 PROTOCOL (T1[0] - FRE) > CONFIG > DLCI MAPPING > BECN TIMEOUT (MSEC)

This value is expressed in milliseconds and represents the amount of time the unit will stop transmitting over a PVC which received a packet with the BECN bit set. Range is **50-5000** msec; the default is **50 SECONDS**.

### L2 PROTOCOL (T1[0] - FRE) > STATUS

View the L2 protocol status for the T1 interface using the Frame Relay protocol.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT

View the Frame Relay statistics on the WAN port.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > PORT INDEX

Integer used for identifying DLCIs on an interface. A single DLCI will always be port index 0. Subsequent DLCIs will have incrementing port indices.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > SIGNAL STATE

Displays “up” when the unit is communicating with the Frame Relay switch; otherwise displays “down”.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > TX FRAMES

Total frames transmitted out the WAN port.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > RX FRAMES

Total frames received from the WAN port.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > TX BYTES

Total bytes transmitted out the WAN port.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > RX BYTES

Total bytes received on the WAN port.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > FULL STATUS TX FRAMES

Number of full status frames transmitted out the WAN port.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > FULL STATUS RX FRAMES

Number of full status frames received on the WAN port

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > LINK INTEGRITY STATUS TX FRAMES

Number of Link-Integrity (LI) only frames transmitted out the WAN port.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > LINK INTEGRITY STATUS RX FRAMES

Number of LI only frames received on the WAN port.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > DROP UNKNOWN DLCI

Number of frames received that were not associated with any known PVC.

### L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > DROP INVALID DLCI

Number of frames received that had illegal DLCIs.

### L2 Protocol (T1[0] - FRE) > Status > Port > Clear Stats

Selecting this activator will clear the port Frame Relay Statistics.

### L2 Protocol (T1[0] - FRE) > Status > PVC's

View the Frame Relay status on a per PVC basis.

### L2 Protocol (T1[0] - FRE) > Status > PVC's > DLCI

The DLCI number identifies the virtual circuit being monitored.

### L2 Protocol (T1[0] - FRE) > Status > PVC's > State

The state of the virtual circuit:

| | |
|---|---|
| **Inactive** | The circuit exists but has been deactivated by the Frame Relay switch. |
| **Exists** | The circuit exists at this point and should be activated soon. |
| **Active** | The circuit is fully active. |
| **Off** | The circuit has been turned off by the DLCI mapping active selection. |

### L2 Protocol (T1[0] - FRE) > Status > PVC's > Tx Frames

Number of Frame Relay packets that have been transmitted via this DLCI.

### L2 Protocol (T1[0] - FRE) > Status > PVC's > Rx Frames

Number of Frame Relay packets that have been received via this DLCI.

### L2 Protocol (T1[0] - FRE) > Status > PVC's > Tx Bytes

Number of Frame Relay bytes that have been transmitted via this DLCI.

### L2 Protocol (T1[0] - FRE) > Status > PVC's > Rx Bytes

Number of Frame Relay bytes that have been received via this DLCI.

### L2 Protocol (T1[0] - FRE) > Status > PVC's > DE Count

Number of packets received on this DLCI with the Discharge Eligible (DE) bit set.

### L2 Protocol (T1[0] - FRE) > Status > PVC's > CR Count

Number of packets received on this DLCI with the Command Response (CR) bit set.

### L2 Protocol (T1[0] - FRE) > Status > PVC's > BECN Count

Number of packets received on this DLCI with the Backward Explicit Congestion Notification (BECN) bit set.

### L2 Protocol (T1[0] - FRE) > Status > PVC’s > FECN Count

Number of packets received on this DLCI with the Forward Explicit Congestion Notification (FECN) bit set.

### L2 Protocol (T1[0] - FRE) > Status > PVC’s > Unknown Frame Rx

Number of frames that have been received that the unit does not know where to route.

### L2 Protocol (T1[0] - Auto)

View the status of the T1 interface with the L2 protocol set to Auto (using Auto-config feature).

### L2 Protocol (T1[0] - Auto) > Status

View the status of the auto detect function and traffic flow for the T1 interface with a L2 protocol set to auto.

### L2 Protocol (T1[0] - Auto) > Status > State

This field represents the state of the auto detect/configuration function. The possible state are:

**Off** The T1 interface is down, so the auto-detect/configuration process is currently idle.

**Detecting L2 Protocol** The T1 interface is up and waiting for the first control/signaling packet.

**Confirming FR** The T1 interface si up and one FR signaling packet has been received

**Confirmed FR** The T1 interface is up and two FR signaling packets have been received. It takes two consecutive control/signaling packets of the same type to confirm the detected protocol.

**Confirming PPP** The T1 interface is up and on PPP control packet has been received.

**Confirmed PPP** The T1 interface is up and two PPP control packets have been received. It takes two consecutive control/signaling packets of the same type to confirm the detected protocol.

### L2 Protocol (T1[0] - Auto) > Status > Tx Pkts

Number of packets transmitted out of the WAN port.

### L2 Protocol (T1[0] - Auto) > Status > Rx Pkts

Number of packets received on WAN port.

### L2 Protocol (T1[0] - Auto) > Status > Tx Bytes

Number of bytes transmitted out of the WAN port.

### L2 PROTOCOL (T1[0] - AUTO) > STATUS > RX BYTES

Number of bytes received out of the WAN port.

### L2 PROTOCOL (T1[0] - AUTO) > STATUS > CLEAR STATS

Selecting the is activator will clear the statistics.

### L2 PROTOCOL (ETH[1])

Configure the **L2 PROTOCOL** parameters and view the status of the Ethernet interface from this menu.

> NOTE *The 1 in ETH[1] represents the physical port. The Ethernet physical port is always 1.*

### L2 PROTOCOL (ETH[1]) > PROTOCOL

Displays the L2 protocol for the 10/100BaseT Ethernet port. Currently only **802.3** is supported.

### L2 PROTOCOL (ETH[1]) > CONFIG

Configure the mode for this **10/100BASET** Ethernet port from this menu.

### L2 PROTOCOL (ETH[1]) > CONFIG > MODE

The mode identifies how the data will be forwarded. The choices are:

| | |
|---|---|
| **ROUTE IP** | All IP data will be routed |
| **BRIDGE ALL** | All data will be bridged |
| **ROUTE IP/BRIDGE OTHER** | All IP data will be routed. All other data will be bridged. |

The default is **ROUTE IP.**

### L2 PROTOCOL (ETH[1]) > STATUS

View the L2 protocol statistics for the **10/100BASET** Ethernet port from this menu.

### L2 PROTOCOL (ETH[1]) > STATUS > TX PACKETS

Total number of packets transmitted out the Ethernet port.

### L2 PROTOCOL (ETH[1]) > STATUS > RX PACKETS

Total number of packets received from the Ethernet port.

### L2 PROTOCOL (ETH[1]) > STATUS > TX ERRORS

Total number of transmit errors encountered on Ethernet port.

### L2 PROTOCOL (ETH[1]) > STATUS > SINGLE COLLISIONS

Total number of single collisions before successful transmission.

### L2 PROTOCOL (ETH[1]) > STATUS > MULTIPLE COLLISIONS

Total number of multiple collisions before successful transmission.

### L2 PROTOCOL (ETH[1]) > STATUS > EXCESSIVE COLLISIONS

Total number of collisions that resulted in packet being dropped.

### L2 PROTOCOL (ETH[1]) > STATUS > DEFERRED TRANSMISSIONS

Total number of packets deferred due to collisions.

### L2 PROTOCOL (ETH[1]) > STATUS > CARRIER SENSE ERRORS

Total number of carrier sense errors encountered (no link integrity).

### L2 PROTOCOL (ETH[1]) > STATUS > RX ERRORS

Number of packets received in error and dropped.

### L2 PROTOCOL (ETH[1]) > STATUS > CRCS

Number of packets detected with CRC errors.

### L2 PROTOCOL (ETH[1]) > STATUS > RX COLLISIONS

Number of collisions which occurred during reception.

### L2 PROTOCOL (ETH[1]) > STATUS > NON-ALIGNED

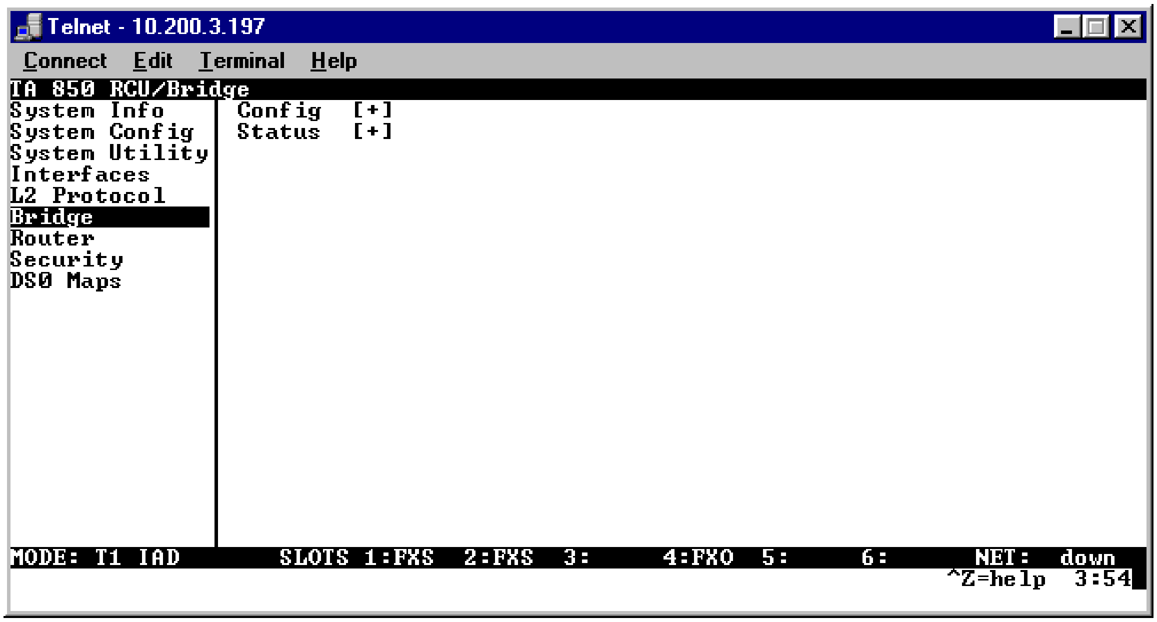
The **NON-ALIGNED** parameter is set when the number of bits received is not divisible by 8.

### L2 PROTOCOL (ETH[1]) > STATUS > CLEAR COUNTS

Selecting this activator clears all the Ethernet stats.

### BRIDGE

Configure the bridge parameters and view bridging statistics from this menu as shown in Figure 7.



```
TA 850 RCU/Bridge
System Info     Config   [+]
System Config   Status   [+]
System Utility
Interfaces
L2 Protocol
Bridge
Router
Security
DS0 Maps

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:        NET:  down
                                                                   ^Z=help  3:54
```

**Figure 7. Bridge Menu**

### BRIDGE > CONFIG

Configure the interfaces and bridge table parameters from this menu.

### BRIDGE > CONFIG > INTERFACES (T1[0])

Configure the T1 interface bridging parameters from this menu.

> NOTE *The T1[0] interface will not appear as a bridge interface entry if the mode is set to route IP.*

### BRIDGE > CONFIG > INTERFACES (T1[0]) > SUB-INTERFACE

The T1 sub-interface is PPP [0.0] if the **L2 PROTOCOL** is set for **PPP**. The [0.0] represents the T1 physical and logical ports respectively. This is a ready-only field. The T1 sub-interface is **FRE [0.X]** if the **L2 PROTOCOL** is set fro **FRAME RELAY**. The [0.X] represents the T1 physical and logical ports respectively. The T1 physical port is always 0. The X represents the Frame Relay logical port and will bed a number between 0-6 corresponding to the interface number under **L2 PROTOCOL > CONFIG > DLCI MAPPING**. This is a read-only field.

### BRIDGE > CONFIG > INTERFACES (ETH[1])

Configure the Ethernet Bridging parameters from this menu.

> *The ETH[1] interface will not appear as a bridge interface entry if the mode is set to route IP.*

### BRIDGE > CONFIG > INTERFACES (ETH[1]) > SUB-INTERFACE

The Ethernet sub-interface is 802.3[1.0] represents the Ethernet physical and logical ports, where 1 is the physical port and 0 is the logical port assigned to the Ethernet interface. This is a read-only field.

### BRIDGE > CONFIG > BRIDGE TABLE

Configure the bridge table parameters from this menu.

### BRIDGE > CONFIG > BRIDGE TABLE > BRIDGE TABLE AGING (0-65535)

**BRIDGE TABLE AGING** is how soon an entry ages out of the Bridge table (in minutes). Default is 5.

### BRIDGE > STATUS

View the bridging statistics from this menu.

### BRIDGE > STATUS > BRIDGE TABLE

View the bridge table status from this menu.

### BRIDGE > STATUS > BRIDGE TABLE > MAC ADDRESS

Ethernet address for device learned. This is a read-only field.

### BRIDGE > STATUS > BRIDGE TABLE > LOCATION

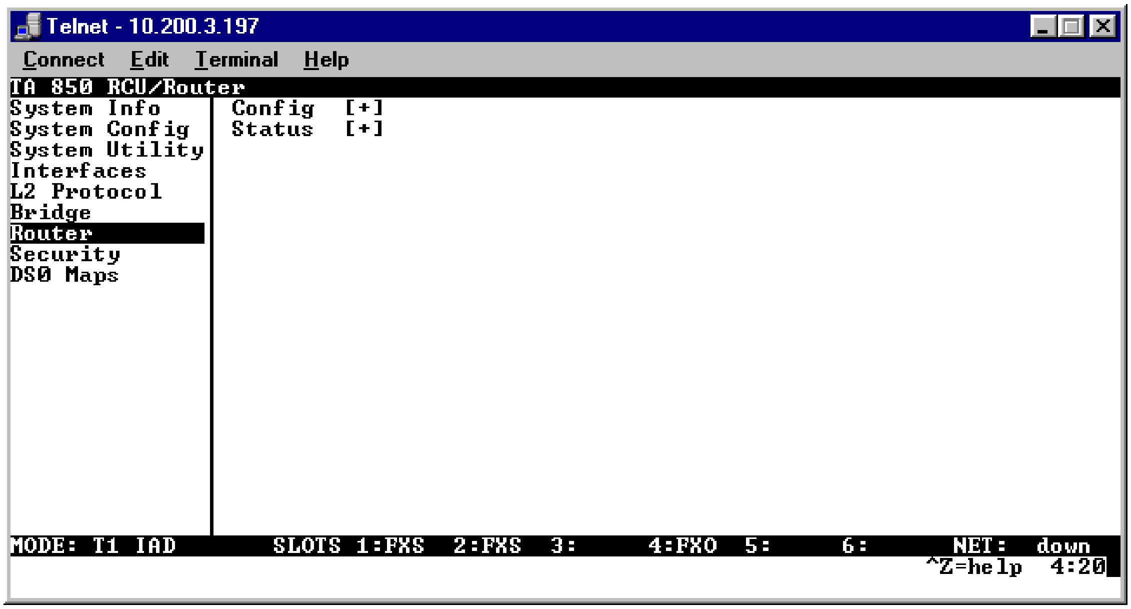
Location indicates if it is LAN or WAN. This is a read-only field.

### BRIDGE > STATUS > BRIDGE TABLE > TTL

Time to Live (TTL) is the number of seconds until the address is removed from the table. This is a read only field.

### ROUTER

Configure the router parameters and view routing statistics from this menu as shown in Figure 8.



```
TA 850 RCU/Router
System Info    Config   [+]
System Config  Status   [+]
System Utility
Interfaces
L2 Protocol
Bridge
Router
Security
DS0 Maps

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:        NET:  down
                                                                   ^Z=help  4:20
```

Figure 8. Router Menu

### ROUTER > CONFIG

Configure the interfaces, routes, DHCP Server, and UDP Relay options from this menu.

### ROUTER > CONFIG > INTERFACES

Configure the layer 3 options for the Ethernet and T1 interfaces from this menu.

### ROUTER > CONFIG > INTERFACES (ETH[1])

Configure the layer 3 options for the Ethernet parameters from this menu.

NOTE *The 1 in ETH[1] represents a physical port. The Ethernet physical port will always be 1.*

NOTE *The Ethernet port will always appear in the* **ROUTER > CONFIG > INTERFACES** *table regardless of the L2 protocol mode setting.*

### ROUTER > CONFIG > INTERFACES (ETH[1]) > SUB-INTERFACE

The Ethernet sub-interface is 802.3[1.0]. The [1.0] represents the Ethernet physical and logical ports, where 1 is the physical port and 0 is the logical port assigned to the Ethernet interface. This is a read-only field.

## ROUTER > CONFIG > INTERFACES (ETH[1])> SETUP

Configure the Ethernet addressing, RIP, and Proxy ARP from this menu.

### PRIMARY IP

This is used to setup the IP addresses for the LAN on the unit.

#### IP ADDRESS

The IP address assigned to the unit's Ethernet port is set here. This address must be unique within the network. Default is **10.0.0.1**.

#### SUBNET MASK

This is the IP network mask that is to be applied to the unit's Ethernet port. Default is **255.255.255.0.**

#### RIP

Use this menu to enable RIP on the LAN interface.

##### VERSION

Enables or disables RIP and specifies the RIP protocol. Choices are; **OFF** (which disables RIP), **V1** (RIP Version 1) or **V2** (RIP Version 2). The default is **OFF**.

##### METHOD

Specifies the way the RIP protocol sends out its advertisements. The following options are available:

| | |
|---|---|
| **SPLIT HORIZON (DEF)** | Only routes not learned from this circuit are advertised. |
| **POISON REVERSE** | All routes are advertised, but the routes learned from this port are "poisoned" with an infinite metric. The default is Split Horizon. |

##### DIRECTION

Allows the direction at which RIP advertisements are sent and received to be specified.

| | |
|---|---|
| **TX AND RX (DEF)** | RIP advertisements are periodically transmitted and are listened to on this port. |
| **TX ONLY** | RIP advertisements are periodically transmitted but are not listened to on this port. |
| **RX ONLY** | RIP advertisements are listened to on this port, but are not transmitted on this port. |

#### V2 SECRET

Enter the secret used by RIP version 2 here.

### PROXY ARP

This feature allows the network portion of a group of addresses to be shared among several physical network segments. The ARP protocol provides a way for devices to create a mapping between physical addresses and logical IP addresses. Proxy ARP makes use of this mapping feature by instructing a router to answer ARP requests as a "proxy" for the IP addresses behind one of its ports. The device which sent the ARP request will then correctly assume that it can reach the requested IP address by sending packets to the physical address that was returned. This technique effectively hides the fact that a network has been (further) subnetted. If this option is set to **YES,** when an ARP request is received on the Ethernet port the address is looked up in the IP routing table. If the forwarding port is not on the Ethernet port and the route is not the default route, the unit will answer the request with its own hardware address. Default is **NO**.

### SECONDARY IPS

This allows the unit to specify additional IP addresses and networks on its Ethernet. The maximum number of entries is 5.

#### NUM

Displays the index number in the secondary IP list.

#### IP ADDRESS

This is the second IP address the unit will respond to on the Ethernet. Default is **0.0.0.0**.

#### SUBNET MASK

This is the mask for the network. Default is **255.255.255.255**.

#### NAT MODE

This mode specifies whether Network Address Translation (NAT) should be use on this interface. When this mode is set to **PRIVATE** (def) NAT is automatically specified on this interface. The other choice is **PUBLIC** which specifies **not** going through NAT.

## ROUTER > CONFIG > ROUTES

Configures the default gateway and static routes from this menu.

## ROUTER > CONFIG > ROUTES > DEFAULT GATEWAY

The default gateway is used by the unit to send IP packets whose destination addresses are not found in the route table. Default is **0.0.0.0.** This is a default gateway for the entire unit, not just for the Ethernet port.

## ROUTER > CONFIG > ROUTES > STATIC ROUTES

Use this menu to enter static routes to other networks.

### NUM

Displays the index number in the static route table.

### ACTIVE

Adds this static route entry to the IP routing table when set to **YES** and removes it (if it was previously added) if set to **NO**. Default is **NO**.

### IP ADDRESS

The IP address of the host or network address of the device being routed to. Default is **0.0.0.0**.

### SUBNET MASK

Determines the bits in the previous IP address that are used. If this is to be a host route, it must be set to all ones (255.255.255.255). Default is **0.0.0.0**.

### GATEWAY

The IP address of the router to receive the forwarded IP packet. Default is **0.0.0.0.**

### HOPS

The number of router hops required to get to the network or host. Maximum distance is 16 hops. Default is **1**.

### PRIVATE

When set to **NO**, the unit will advertise this static route using RIP. Setting to **YES** means that the route is kept private. Default is **NO**.

## ROUTER > CONFIG > DHCP SERVER

Use this menu to set up the DHCP server.

## ROUTER > CONFIG > DHCP SERVER > DHCP MODE

When set to **ON**, the unit acts as a DHCP server and will dynamically assign IP, network mask, default gateway, and DNS addresses to any device which transmits a broadcast DHCP request. The addresses assigned are based on the unit's own IP address and will be within the same network. Default is **OFF.**

## ROUTER > CONFIG > DHCP SERVER > DHCP RENEWAL TIME (HOURS)

The number of hours that the DHCP server should allow the device to keep its previous IP assignment, before it is required to send a new DHCP request. The default is **0 HOURS** which represents an infinite lease.

### ROUTER > CONFIG > DHCP SERVER > DOMAIN NAME

Text string used to represent the domain name used by the unit.

### ROUTER > CONFIG > DHCP SERVER > PRIMARY DNS

First server to which domain name requests are sent.

Default is 0.0.0.0.

### ROUTER > CONFIG > DHCP SERVER > SECONDARY DNS

Server used as a backup, in case the primary address does not respond to the request.

Default is 0.0.0.0.

### ROUTER > CONFIG > DHCP SERVER > PRIMARY NBNS/WINS

Primary address of the NBNS/WINS server.

Default is 0.0.0.0.

### ROUTER > CONFIG > DHCP SERVER > SECONDARY NBNS/WINS

Secondary address of the NBNS/WINS server.

Default is 0.0.0.0.

### ROUTER > CONFIG > UDP RELAY

This menu configures the unit to act as a UDP relay agent for applications requiring a response from UDP hosts that are not on the same network segment as their clients.

### ROUTER > CONFIG > UDP RELAY > MODE

When this option is set to **ON**, the unit will act as a relay agent. Default is **OFF**.

### ROUTER > CONFIG > UDP RELAY > UDP RELAY LIST

Up to four relay destination servers can be specified in this list.

#### #

Indicates the entry number in the UDP Relay List table.

#### RELAY ADDRESS

This is the IP address of the server that will receive the relay packet. Default is **0.0.0.0**.

### UDP PORT TYPE

The choices are **STANDARD** (def) and **SPECIFIED**. The following standard UDP protocols are relayed when set: DHCP, TFTP, DNS, NTP (Network Time Protocol, port 123), NBNS (NetBios Name Server, port 137), NBDG (NetBIOS Datagram, port 138), and BootP. When **SPECIFIED** is set, the UDP port (1 to 65535) can be specified in the UDP Port columns (up to three per server).

### UDP PORT 1, 2, 3

Used for specifying UDP ports to be relayed. These fields only apply when **UDP PORT TYPE** is set to **SPECIFIED**. Default is **0**.

## ROUTER > STATUS

View the **IP ROUTES**, **IP STATS**, and **ARP CACHE** statistics from this menu.

## ROUTER > STATUS > IP ROUTES

This lists the contents of the unit's IP route table.

## ROUTER > STATUS > IP ROUTES > IP ADDRESS

Network or host destination address.

## ROUTER > STATUS > IP ROUTES > NETMASK

Network mask applied to the destination address.

## ROUTER > STATUS > IP ROUTES > GATEWAY

Host or router to receive this packet.

## ROUTER > STATUS > IP ROUTES > PORT

Port gateway is located on:

| | |
|---|---|
| **LOCAL** | Sent directly to the unit's router |
| **ETH0** | The unit's Ethernet port |
| **WAN0** | The unit's first PPP bundle |
| **FR 0 . . . FR 9** | The unit is connected up to 10 DLCIs |

## ROUTER > STATUS > IP ROUTES > USE

Number of times the unit has referenced the route.

### ROUTER > STATUS > IP ROUTES > FLAGS

Important tags associated with this route entry

| | |
|---|---|
| **H** | route is a host route |
| **G** | route is a gateway route |
| **S** | static route, or learned via IPCP, IARP, DHCP |
| **R1** | learned from RIP Version 1 |
| **R2** | learned from RIP Version 2 |
| **I** | route learned from an ICMP redirect |
| **C** | directly connected interface |
| **P** | route is private and is not advertised with RIP |
| **T** | route is to a triggered port (updates only when table changes) |
| **U** | learned by unknown method |

### ROUTER > STATUS > IP ROUTES > HOPS

Number of routers that must go through to get to destination. Ranges from 0-15 or 16 for infinite (can't get there from here).

### ROUTER > STATUS > IP ROUTES > TTL

Seconds until address is removed from table. Value of 999 means route is static.

### ROUTER > STATUS > IP STATS

This section describes the following **STATISTICS** submenus (and see the tables on the pages following):

- IP
- ICMP
- TCP
- UDP

All of these statistics are taken from the MIB-II variables in RFC 1156. To clear the accumulated statistics, press the **<ENTER>** key on **CLEAR COUNTS**.

### ROUTER > STATUS > IP STATS > IP

View the IP statistics from this menu.

### DEFAULT TTL

The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this unit, whenever a TTL value is not supplied by the transport layer protocol.

### IP DATAGRAMS RECEIVED

The total number of input datagrams received from interfaces, including those received in error.

### BAD HEADER PACKETS

The number of input datagrams discarded due to errors in their IP headers, including bad check sums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

### BAD IP ADDRESSES

The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this unit. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

### TOTAL FORWARDED DATAGRAMS

The number of input datagrams for which this unit was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this unit, and the Source-Route option processing was successful.

### BAD PROTOCOL DISCARDS

The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

### DATAGRAMS DISCARDED

The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

### SENT DATAGRAMS TO UPPER LAYERS

The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

### IP DATAGRAMS SENT

IP packets from the unit's IP stack.

#### ERRORFREE DISCARDS

The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in **TOTAL FORWARDED DATAGRAMS** if any such packets met this (discretionary) discard criterion.

#### ROUTELESS DISCARDS

The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in **TOTAL FORWARDED DATAGRAMS** which meet this “no-route” criterion. Note also that this includes any datagrams which a host cannot route because all of its default gateways are down.

#### IP REASSEMBLY TIMEOUT

The maximum number of seconds received fragments are held while awaiting reassembly at this unit.

#### DISASSEMBLED FRAGMENTS

The number of IP fragments received which needed to be reassembled at this unit.

#### IP DATAGRAMS REASSEMBLED

The number of IP datagrams successfully reassembled.

#### IP REASSEMBLY FAILURES

The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably RFC 815s) can lose track of the number of fragments by combining them as they are received.

#### SUCCESSFUL FRAGMENTS

The number of IP datagrams that have been successfully fragmented at this unit.

#### FAILED FRAGMENTS

The number of IP datagrams that have been discarded because they needed to be fragmented at this unit but could not be e.g., because their “Don't Fragment” flag was set.

#### TOTAL IP FRAGMENTS

The number of IP datagram fragments that have been generated as a result of fragmentation at this unit.

### DISCARDED ROUTING ENTRIES

A packet the unit couldn't route.

### CLEAR COUNTS

Setting this activator clears the IP Statistics.

## ROUTER > STATUS > IP STATS > ICMP

### ICMP MESSAGES RECEIVED

The total number of ICMP messages the unit received. Note that this counter includes all those counted by **ICMP SPECIFIC ERRORS**.

### ICMP SPECIFIC ERRORS

The number of ICMP messages the unit received but determined as having errors (bad ICMP checksums, bad length, etc.)

### ICMP DEST. UNREACHABLE MSGS RCVD

The number of ICMP Destination Unreachable messages received.

### ICMP TIMEOUTS RECEIVED

The number of ICMP Time Exceeded messages received.

### ICMP PARAMETER PROBLEM MSGS RCVD

The number of ICMP Parameter Problem messages received.

### ICMP SOURCE QUENCH MSGS RCVD

The number of ICMP Source Quench messages received.

### ICMP REDIRECTED MESSAGES RCVD

The number of ICMP Redirect messages received.

### ICMP ECHO REQUEST MSGS RCVD

The number of ICMP Echo (request) messages received.

### ICMP ECHO REPLY MSGS RCVD

The number of ICMP Echo Reply messages received.

### ICMP Timestamp Request Msgs Rcvd

The number of ICMP Timestamp (request) messages received.

### ICMP Timestamp Reply Msgs Rcvd

The number of ICMP Timestamp Reply messages received.

### ICMP Address Mask Request Msgs Rcvd

The number of ICMP Address Mask Request messages received.

### ICMP Address Mask Reply Msgs Rcvd

The number of ICMP Address Mask Reply messages received.

### ICMP Messages Sent

The total number of ICMP messages this unit attempted to send. Note that this counter includes all those counted by **ICMP Packet Errors.**

### ICMP Packet Errors

this unit did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.

### ICMP Dest. Unreachable Msgs Sent

The number of ICMP Destination Unreachable messages sent.

### ICMP Time Eceeded Msgs Sent

The number of ICMP Time Exceeded messages sent.

### ICMP Parameter Problem Msgs Sent

The number of ICMP Parameter Problem messages sent.

### ICMP Source Quench Msgs Sent

The number of ICMP Source Quench messages sent.

### ICMP Redirect Msgs Sent

The number of ICMP Redirect messages sent.

#### ICMP Echo Request Msgs Sent

The number of ICMP Echo (request) messages sent.

#### ICMP Echo Reply Msgs Sent

The number of ICMP Echo Reply messages sent.

#### ICMP Timestamp Request Msgs Sent

The number of ICMP Timestamp (request) messages sent.

#### ICMP Timestamp Reply Msgs Sent

The number of ICMP Timestamp Reply messages sent.

#### ICMP Addr Mask Request Msgs Sent

The number of ICMP Address Mask Request messages sent.

#### ICMP Addr Mask Reply Msgs Sent

The number of ICMP Address Mask Reply messages sent.

#### Clear Counts

Selecting this activator will clear the ICMP statistics.

### Router > Status > IP Stats > UDP

View the UDP statistics from this menu.

#### UDP Datagrams Received

The total number of UDP datagrams delivered to UDP users.

#### No Application at Dest. Port

The total number of received UDP datagrams for which there was no application at the destination port.

#### UDP Bad Packets

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

#### UDP Datagrams Sent

The total number of UDP datagrams sent from this unit.

#### CLEAR COUNTS

Selecting this activator clears the UDP statistics.

### ROUTER > STATUS > IP STATS > UDP TABLE

View the UDP table statistics from this menu.

#### LOCAL IP ADDRESS

The destination IP address of the packet

#### PORT

The destination UDP port of the packet.

### ROUTER > STATUS > IP STATS > TCP

View the TCP statistics from this menu.

#### RETRANSMISSION TIMEOUT ALGORITHM

The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.

#### MIN RETRANSMISSION TIMEOUT (MS)

The minimum value permitted by a **TCP** implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the **LBOUND** quantity described in RFC 793.

#### MAX RETRANSMISSION TIMEOUT (MS)

The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the **UNBOUND** quantity described in RFC 793.

#### MAX TCP CONNECTIONS

The limit on the total number of **TCP** connections the unit can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

#### ACTIVE TCP CONNECTIONS

The number of times **TCP** connections have made a direct transition to the **SYN-SENT** state from the **CLOSED** state.

### TCP PASSIVE CONNECTIONS

The number of times **TCP** connections have made a direct transition to the **SYN-RCVD** state from the **LISTEN** state.

### TCP FAILED ATTEMPTS

The number of times **TCP** connections have made a direct transition to the **CLOSED** state from either the **SYN-SENT** state or the **SYN-RCVD** state, plus the number of times **TCP** connections have made a direct transition to the **LISTEN** state from the **SYN-RCVD** state.

### TOTAL TCP RESETS

The number of times TCP connections have made a direct transition to the **CLOSED** state from either the **ESTABLISHED** state or the **CLOSE-WAIT** state.

### TCP CURRENT CONNECTIONS

The number of TCP connections for which the current state is either **ESTABLISHED** or **CLOSE-WAIT**.

### TCP SEGMENTS RECEIVED

The total number of segments received, including those received in error. This count includes segments received on currently established connections.

### TCP SEGMENTS SENT

The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

### TOTAL TCP RETRANSMITS

The total number of segments retransmitted -- that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

### CLEAR COUNTS

Selecting this activator clears the TCP statistics.

## ROUTER > STATUS > IP STATS > TCP CONNS

View the TCP Conns Statistics from this menu. This table shows the different states of each TCP connection.

### STATE

The possible states are **FREE**, **CLOSED**, **LISTEN**, **SYNC SENT**, **SYNC RECEIVED**, **ESTABLISHED**, **FINWAIT1**, **FINWAIT2**, **CLOSEWAIT**, **LASTACK**, **CLOSING**, and **TIMEWAIT**.

### LOCAL IP ADDRESS

Local IP address of the TCP connection.

### LOCAL PORT

Local port of the TCP connection.

### REMOTE IP ADDRESS

Remote IP address of the TCP connection.

### REMOTE PORT

Remote port of the TPC connection.

## ROUTER > STATUS > IP STATS > ARP CACHE

This lists the contents of the units's ARP table. All resolved cache entries time out after 20 minutes. Unresolved entries time out in 3 minutes. The ARP cache can be cleared by pressing "**f**" while on the menu or by pressing "**d**" on the individual number for that entry.

### IP ADDRESS

IP address used for resolving MAC address.

### MAC ADDRESS

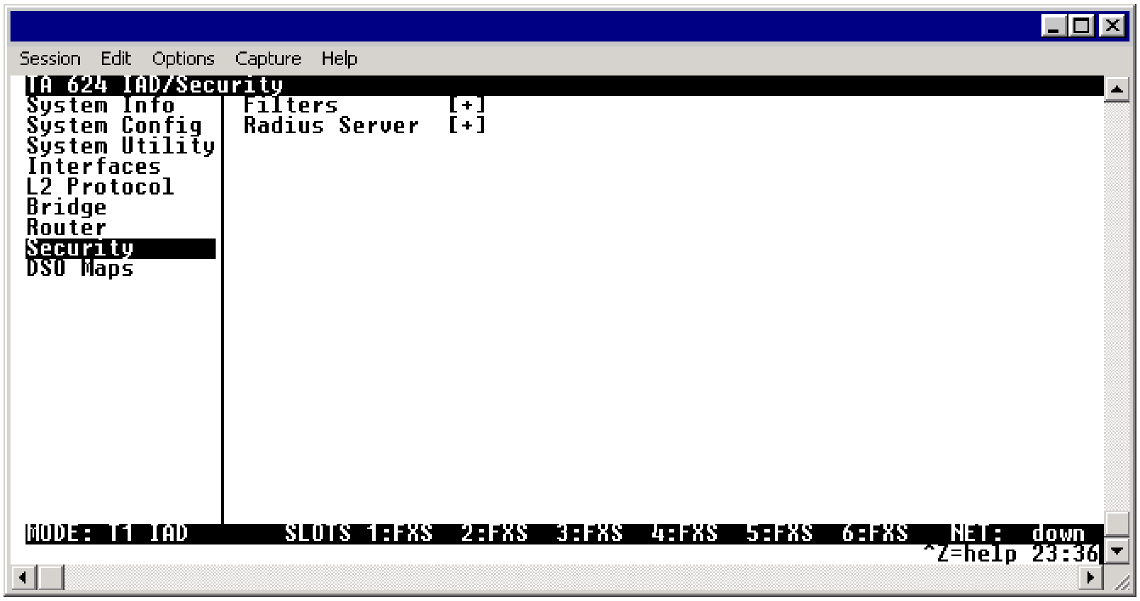
Ethernet address resolved (0=no resolution).

### TIME

Minutes since entry was first entered.

## SECURITY

Configure the **SECURITY FILTERS** and **RADIUS SERVER** parameters from this menu as shown in Figure 9.



```
TA 624 IAD/Security
System Info      Filters        [+]
System Config    Radius Server  [+]
System Utility
Interfaces
L2 Protocol
Bridge
Router
Security
DS0 Maps

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:FXS  4:FXS  5:FXS  6:FXS    NET:  down
                                                                  ^Z=help 23:36
```

**Figure 9. Security Menu**

## SECURITY > FILTERS

Configure the filter characteristics from this menu.

## SECURITY > FILTERS > FILTER DEFINES

The unit can filter packets based on certain parameters within the packet. The method used by the unit allows the highest flexibility for defining filters and assigning them to a PVC or PPP link. The filters are set up in two steps: (1) defining the filter types, and (2) applying them to a list under the PVC or PPP configuration. This menu is used to define the individual filter defines based on packet type.

NOTE *The Filter Defines option works for Frame Relay and PPP.*

## SECURITY > FILTERS > FILTER DEFINES > MAC FILTER DEFINES

The MAC filter is applied to bridge packets only. Bridge packets which are forwarded by the bridge functionality of the unit are defined here. Up to 32 MAC defines can be specified.

### NUM

Indicates the entry number in the MAC Filter Defines table.

#### NAME

Identifies the filter entry. Default is no entry in **NAME** field.

#### SRC ADDR

48-bit MAC source address used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

#### SRC MASK

Bits in the MAC source address which are compared. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

#### DEST ADDR

48-bit MAC destination address used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

#### DEST MASK

Bits in the MAC destination address used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

#### TYPE

16-bit type field used for comparison. Values are in hexadecimal format. Default is **00:00**.

#### TYPE MASK

Bits in the type field used for comparison. Values are in hexadecimal format. Default is **00:00**.

### SECURITY > FILTERS > FILTER DEFINES > PATTERN FILTER DEFINES

The pattern filter is applied to bridge packets only. That is any packet which is forwarded by the bridge functionality of the unit. Up to 32 pattern defines can be specified.

#### NUM

Indicates the entry number in the Pattern Filter Defines table.

#### NAME

Identifies the filter entry. Default is no entry in **NAME** field.

#### OFFSET

Offset from beginning of packet of where to start the pattern comparison. Default is **0**.

#### PATTERN

64 bits used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00:00:00**.

#### MASK

Bits in the pattern to be compared. Values are in hexadecimal format. Default is **00:00:00:00:00:00:00:00**.

### SECURITY > FILTERS > FILTER DEFINES > IP FILTER DEFINES

The IP filter defines apply to any IP packet, whether it is routed or bridged. Up to 32 IP defines can be specified.

#### NUM

Indicates the entry number in the IP Filter Defines table.

#### NAME

Identifies the filter entry. Default is no entry in name field.

#### SRC ADDR

IP address compared to the source address. Value is in dotted decimal format. Default is **0.0.0.0**.

#### SRC MASK

Bits which are used in the source comparison. Value is in dotted decimal format. Default is **0.0.0.0**.

#### DEST ADDR

IP address compared to the destination address. Value is in dotted decimal format. Default is **0.0.0.0.**

#### DEST MASK

Bits which are used in the destination comparison. Value is in dotted decimal format. Default is **0.0.0.0.**

#### SRC PORT

IP source port number used for comparison. Value is in decimal format. Range: **0 TO 65535**. Default is **0**.

### SRC PORT COMP

Type of comparison that is performed. Default is **NONE**.

**=** means ports equal to

**NOT =** means port not equal to

**>** means port greater than

**<** means port less than

**None** - means the source port is not compared

### DEST PORT

IP destination port number used for comparison. Value is in decimal format. Range: **0 TO 65535**. Default is **0**.

### DEST PORT COMP

Type of comparison that is performed. Default is **NONE**.

**=** means ports equal to

**NOT =** means port not equal to

**>** means port greater than

**<** means port less than

**None** - means the source port is not compared

### PROTO PORT

Protocol used for comparison. Value is in decimal format. Range: **0 TO 255**. Default is **0**.

### PROTO PORT COMP

Type of comparison that is performed. Default is **NONE**.

**=** means ports equal to

**NOT =** means port not equal to

**>** means port greater than

**<** means port less than

**None** - means the source port is not compared

#### TCP ESTAB

**Yes** - only when TCP established

**No** - only when TCP not established

**Ignore** - ignore TCP flags (default)

### SECURITY > FILTERS > INTERFACES

The unit can block packets in and out of an interface by use of the filters. They are set up in two steps: 1) define the types of packets that would be of interest in the **SECURITY > FILTERS > FILTER DEFINES** menu, and 2) set up the filter type and combination of defines that will cause a packet block.

### SECURITY > FILTERS > INTERFACES (ETH[1])

Define the filters for the Ethernet interface from this menu.

### SECURITY > FILTERS > INTERFACES (ETH[1]) > SUB-INTERFACE

The Ethernet sub-interface is 802.3[1.0]. This is a read-only field.

### SECURITY > FILTERS > INTERFACES (ETH[1]) > SET-UP

Enable the Ethernet interface filtering and define filters from this menu.

#### IN FROM VC

The packets which come into the unit can be filtered in three ways:

**DISABLE (DEF)** Turns off packet input filtering. No incoming packets are blocked.

**BLOCK ALL** All incoming packets from the WAN are blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > IN EXCEPTIONS** list.

**FORWARD ALL** All incoming packets from the WAN are not blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > IN EXCEPTIONS** list.

#### IN EXCEPTIONS

This is a list of up to 32 filter entries which can be combined using the operations field. The operations are performed in the order they appear on the list.

#### #

Indicates the entry number in the In Exceptions table.

#### ACTIVE

Turns this entry active when set to **YES**. Default is **NO**.

#### TYPE

Selects the filter define list to reference (default is **MAC**).

| | |
|---|---|
| **MAC** | from the **SECURITY > FILTERS > FILTER DEFINES > MAC FILTER DEFINES** list. |
| **PATTERN** | from the **SECURITY > FILTERS > FILTER DEFINES > PATTERN FILTER DEFINES** list. |
| **IP** | from the **SECURITY > FILTERS > FILTER DEFINES > IP FILTER DEFINES** list. |

#### FILTER LIST NAME

Selects between filters defined in the list. Default is no entry in filter list name.

#### NEXT OPER

The next operation to use to combine with the next filter in the list (default is **END**).

| | |
|---|---|
| **END** | the last filter to combination. |
| **AND** | logically AND this filter with the next filter in the list. |
| **OR** | logically OR this filter with the next filter in the list. |

#### OUT TO VC

The packets which come from the unit to the WAN can be filtered in three ways:

| | |
|---|---|
| **DISABLE (DEF)** | Turns off packet outputs filtering. No outgoing packets are blocked. |
| **BLOCK ALL** | All outgoing packets to the WAN are blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > OUT EXCEPTIONS** list. |
| **FORWARD ALL** | All outgoing packets to the WAN are not blocked except as defined in the **SECURITY > FILTERS > INTERFACES > INTERFACES > SETUP > OUT EXCEPTIONS** list. |

#### OUT EXCEPTIONS

This is a list of up to 32 filter entries which can be combined using the operations field. The operations are performed in the order they appear on the list.

#### #

Indicates the entry number in the In Exceptions table.

#### ACTIVE

Turns this entry active when set to Ye**S**. Default is N**O**.

#### TYPE

Selects the filter define list to reference (default is **MAC**):

**MAC** from the **SECURITY > FILTERS > FILTER DEFINES > MAC FILTER DEFINES** list.

**PATTERN** from the **SECURITY > FILTERS > FILTER DEFINES > PATTER FILTER DEFINES** list.

**IP** from the **SECURITY > FILTERS > FILTER DEFINES > IP FILTER DEFINES** list.

#### FILTER LIST NAME

Selects between filters defines in the list. Default is no entry in filter list name.

#### NEXT OPER

The next operation to use to combine with the next filter in the list (default is **END**):

**END** the last filter to combination.

**AND** logically AND this filter with the next filter in the list.

**OR** logically OR this filter with the next filter in the list.

### SECURITY > RADIUS SERVER

The parameters for the R**ADIUS SERVER** are configured in this menu.

> NOTE *Telnet radius is only available in A.04 firmware or late.*

### SECURITY > RADIUS SERVER > SERVER 1

This is the IP address of the first **RADIUS SERVER** that the unit should attempt to communicate with when authenticating a telnet session. Default is **0.0.0.0**.

### SECURITY > RADIUS SERVER > SERVER 2

This is the IP address of the second **RADIUS SERVER** that the unit should attempt to communicate with when the primary server does not respond. Default is **0.0.0.0**.

### SECURITY > RADIUS SERVER > SERVER 3

This is the IP address of the third **RADIUS SERVER** that the unit should attempt to communicate with when the primary server does not respond. Default is **0.0.0.0**.

### SECURITY > RADIUS SERVER > UDP PORT

This is the IDP port the unit should use when communicating with the **RADIUS SERVER**. The default is **1812**, which the commonly used port.

### SECURITY > RADIUS SERVER > SECRET

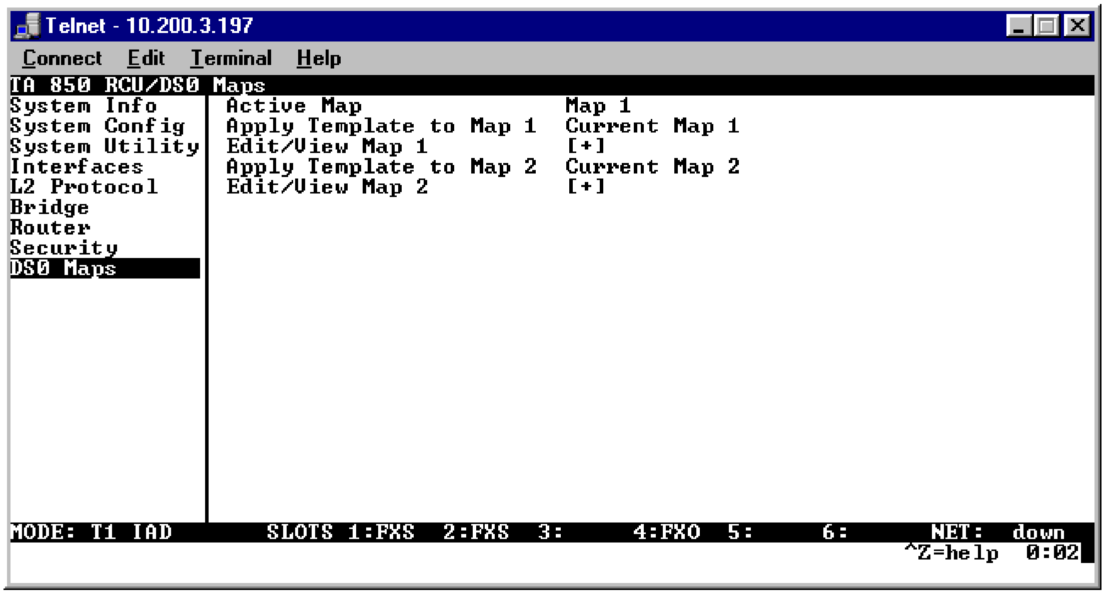
The R**ADIUS SERVER** and unit share this text string. It is used by the **RADIUS SERVER** to authenticate the unit, the RADIUS client. The factory default is not to use a secret.

### SECURITY > RADIUS SERVER > RETRY COUNT (1-10)

This is the number of times the unit should send a request packet tho the **RADIUS SERVER** without a response before giving up. If the number of attempts to communicate with the primary server is equal to the retry count, the second server (if defined) is tried. If the second server does not respond within the retry count the third server (if defined) is tried. If the third server does not respond within the retry count, the Telnet session is not authenticated and is dropped. The default is **5**.

## DS0 MAPS

The **DS0 MAPS** menu allows you to map data and voice ports to the network T1 time slots. You may edit either of the two maps at any time. If you make changes to the current map, only those DS0s that have changed will be updated (unchanged DS0s will not be affected.) The DS0 menu is shown in Figure 10.



```
TA 850 RCU/DS0 Maps
System Info     Active Map               Map 1
System Config   Apply Template to Map 1  Current Map 1
System Utility  Edit/View Map 1          [+]
Interfaces      Apply Template to Map 2  Current Map 2
L2 Protocol     Edit/View Map 2          [+]
Bridge
Router
Security
DS0 Maps

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET:  down
                                                                  ^Z=help  0:02
```

**Figure 10. DS0 Maps Menu**

## DS0 Maps > Active Maps

Activates one of the two dedicated maps (**Map 1** or **Map 2**), or the **Dual T1 Map**. In the **Dual T1 Mode**, the built-in DSX-1 interface DSX[3] can be utilized as a secondary T1 connection. In **Dual T1 Mode**, the second T1 is limited to voice. For example, the user may map all 24 DS0s on the network T1 to the router and on the second T1 (DSX-1 interface) map all 24 DS0s to the FXS cards. Default is **Map 1**.

## DS0 Maps > Apply Template to Map 1

Choices are **Current Map 1**, **Current Map 2**, **D4 Map**, **D1D Map**, **Full Router** and **Clear Map**. Default is **Current Map 1**. **D4 Map** automaps the voice port in a 1-to-1 configuration. D1D Map maps voice ports in an SLC-96 configuration. **Full Router** maps all 24 DS0s to the router at 64K. **Clear Map** clears the entire map.

## DS0 Maps > Edit/view Map 1

Define map 1. The map allows the user to assign services and ports to the individual DS0s 1-24.

NOTE *In the default configuration for TDM A.04.XX firmware, DS0 24 is mapped to the router at 64K on Map 1.*

## DS0 Maps > Edit/View Map 1 > DS0

Displays the network T1 time slot to be assigned.

### DS0 MAPS > EDIT/VIEW MAP 1 > SLOT

When you select this option, a list of all of the slots and the modules displays. This first option **OPEN**, when unassigns the slot if selected. For modules, the slot number and name are shown. For example, **FXS** indicates that an FXS card is installed. Use **TA IAD** to map network timeslot to the **V.35** port or to the router. Pick the appropriate Server and press **<ENTER>**. Default is **OPEN**.

### DS0 MAPS > EDIT/VIEW MAP 1 > PORT

When you select this option, a list of ports appears. Pick the appropriate port, and press **<ENTER>**. The selection list shows only the remaining ports available to be assigned. It may be necessary to unassign a port in order to reassign it elsewhere.

### DS0 MAPS > EDIT/VIEW MAP 1 > RBS

Robbed Bit Signaling. Default is **N/A**. Once a **SLOT** and port are assigned, this will automatically change to **ON** or **OFF**. The unit automatically assigns **OFF** where **RBS** is not an option. **ON** preserves the signaling bits between the connections. **OFF** ignores the signaling bits. For the **FXS**, **RBS** defaults to **ON**. The **RBS** parameter remains at **N/A** for the **TA IAD**, because **RBS** is not applicable to data connections.

> NOTE *Map 2 menus are identical to Map 1. Please use the menu explanations above for Map 2.*

# Appendix A. Configuring the Unit for Routing

## *Initial Setup*

Before the unit can be configured for routing, the DS0s must be mapped.

## *DS0 Mapping*

| **DS0 Mapping Instructions** | |
|---|---|
| **Step** | **Action** |
| **1.** | From the Main menu, select **DS0 MAPS**. |
| **2.** | Verify that the **ACTIVE  MAP** is set to either **MAP 1** or **MAP 2**. This is the map that is actively running on the unit. The unit has the ability to store two maps.<br>• To edit the current map, press **ENTER** on **EDIT/VIEW MAP 1** to view the map. (If Map 1 is the Active Map)<br>• To edit the standby map, press **ENTER** on **EDIT/VIEW MAP 2** to view the map. (If Map 2 is the Active Map) |
| NOTE | *The T1 line entering the unit is broken up into 24 DS0s or channels. At least one DS0 needs to be mapped to the router in order to use the unit for routing purposes.* |
| **3.** | Scroll down to the DS0 that will be mapped. (Any DS0 can be mapped to the router.) |
| **4.** | Set the **SLOT** for the DS0 that you are mapping to **TA IAD**. |
| **5.** | Set the **PORT** of the DS0 that you are mapping to **ROUTER 64K** or **ROUTER 56K**. |
| **6.** | Map all the DS0s as desired, and exit this menu by pressing the left arrow button. Your changes will automatically save when exiting the map. |
| **7.** | Make sure the **ACTIVE MAP** is set to the correct map (the map you want running) before exiting the **DS0 MAPS** menu. |

## *Setting up Routing Options*

The unit can support IP routing and bridging. These procedures are described on the pages that follow.

## *IP Routing*

After completing the DS0 mapping, there are three remaining steps required for the unit to be used for IP Routing: (1) Ethernet Interface Configuration, (2) T1 Interface Configuration, and (3) Default Gateway Configuration. All of these procedures are described in the pages that follow.

### Router Ethernet Interface Setup

| Router Ethernet Interface Setup Instructions | |
|---|---|
| **Step** | **Action** |
| **1** | From the Main Menu, select **ROUTER**, select **CONFIG**, select **INTERFACES** and then select **ETH [1] SETUP** and press **ENTER**. |
| **2** | Press **Enter** on the **PRIMARY IP [+]** option to enter primary Ethernet configuration. |
| **3** | Set the **IP ADDRESS** of the Ethernet port. |
| **4** | Set the **SUBNET MASK** of the Ethernet port. |
| **5** | **RIP** on the Ethernet is disabled by default. If **RIP** needs to be enabled, press **Enter** on **RIP** [+]. |
| **6** | Press **ENTER** on **VERSION** and select **V1** or **V2** to activate **RIP**. |
| **7** | Press the down arrow and select the appropriate **RIP METHOD**, **DIRECTION**, and **V2 SECRET** (where applicable). |
| **8** | Press the left arrow key to return to the Ethernet menu showing **PRIMARY IP** and **SECONDARY IPS**. |
| **9** | If the unit needs additional secondary IP addresses, press **Enter** on **SECONDARY IPS** [+].The unit supports up to 5 additional LAN segments.<br>Enter each additional secondary IP address and subnet mask. Press "I" to insert additional entries. |

### Router T1 Interface Setup

Before configuring the Router T1 Interface, choose **L2 PROTOCOL** and select **PPP**, **FRE**, or **AUTO**. Setup instructions for the **PPP** and **FRE** are described on the following pages. For information on setting the **L2 PROTOCOL** to **AUTO**.

| Router T1 Interface Setup Instructions when L2 Protocol = PPP | |
|---|---|
| **Step** | **Action** |
| **1** | From the main menu, select **L2 PROTOCOL** and press **ENTER**. |
| **2** | Set the T1 [0] interface protocol to **PPP.** |
| **3** | Press **Enter** on the **CONFIG [+]** option. Verify mode is Route IP. |

**Router T1 Interface Setup Instructions when L2 Protocol = PPP**

| | |
|---|---|
| **4** | Press **Enter** on the **AUTHENTICATION [+]** option if you wish to change options related to how the link is established. Default is **TX METHOD = NONE** and **RX METHOD = NONE**. If **TX METHOD** and **RX METHOD** are set to any option other than **NONE**, **TX/RX USERNAME** and **PASSWORD** options will appear. |
| **5** | Left arrow back to the main menu. |
| **6** | Select router, select **CONFIG**, select **INTERFACES**, and select **T1 [0] SETUP**. Enter WAN information:<br>• Far-End IP Address The far-end WAN IP address from the unit.<br>• IP Netmask The subnet mask for this WAN link<br>• Local IP Address The local WAN IP address for the unit.<br>The other config items can be left at the defaults. |
| **7** | For **NAT** configuration, please see the **IP Routing with NAT** section of this appendix on page 141. |

**Router T1 Interface Setup Instruction when L2 Protocol = Frame Relay (FRE)**
(required if the unit is to be used for Frame Relay IP Routing on the WAN interface)

| Step | Action |
|---|---|
| **1** | From the main menu, select **L2 PROTOCOL** and press **ENTER**. |
| **2** | Set the **T1 [0]** interface protocol to **FRE**. |
| **3** | Press **Enter** on the **CONFIG [+]** option. |
| **4** | Set the **MAINTENANCE PROTOCOL** to **ANNEX D** (ANSI)**, ANNEX A** (q 933a)**, LMI, OR STATIC** (no sig). |
| NOTE | *The* **MAINTENANCE PROTOCOL** *should be set based on the Frame Relay switch.* |
| **5** | Down arrow and press **Enter** on **DLCI MAPPING [+]**. Right arrow one time to create an entry. |
| **6** | Set **ACTIVE** to **YES**. |
| **7** | Set **DLCI** to the DLCI number. |
| **8** | Set mode to **ROUTE IP**. |

| **Router T1 Interface Setup Instruction when L2 Protocol = Frame Relay (FRE)**<br>(required if the unit is to be used for Frame Relay IP Routing on the WAN interface) | |
|---|---|
| **9** | Left arrow back to the main menu. Select **ROUTER**, select **CONFIG**, select **INTERFACES**, and select **T1 [0] SETUP**. Set **ACTIVE** to **YES**. |
| **10** | Set **ADDRESS MODE** to **USER SPECIFIED** and enter a **FAR-END IP ADDRESS**. This will force the unit to not use IARP. |
| **11** | Enter the IP Netmask. |
| **12** | Enter the local IP address for the unit. The other config items can be left at the default values. |
| **13** | For **NAT** configuration, please see the **IP Routing with NAT** section of this appendix on page 141. |

| **Router T1 Interface Setup Instructions - IP Routing with NAT** | |
|---|---|
| **Step** | **Action** |
| **1** | The **NAT** menu is found under **Router >Config >Interfaces (T1 [0]) > Setup**. The **NAT** menu can be easily accessed by pressing **<Ctrl><N>**. |
| NOTE | *The T1 interface will not appear if a DLCI is not entered in the DLCI mapping table* **(L2 PROTOCOL T1[0]-FRE > CONFIG > DLCI MAPPING)** *when the L2 protocol is set to Frame Relay (FRE).* |
| **2** | From the **NAT** menu, set **PORT TRANSLATION** to **ENABLED**. (This will enable translation and populate the corresponding **NAT** menu options.) |
| **3** | Set **PUBLIC IP ADDRESS MODE** to either **INTERFACE** or **SPECIFIED**.<br>• **INTERFACE** is the default and will use the WAN IP address for the NAPT address.<br>• **SPECIFIED** allows you to enter another public address for private addresses to be translated into.<br>For basic **NAT**, this is all of the configuration that needs to be done.<br>For specific port translations or 1:1 mapping, you can enter **TRANSLATION TABLE** [+]. |

| Router T1 Interface Setup Instructions - IP Routing with NAT | |
|---|---|
| **4** | From the **TRANSLATION TABLE** menu, create a new entry by using the right arrow to enter the table. |
| **5** | Create specific **NAT** translations based on your application.<br>**PUBLIC ADDRESS MODENAPT ADDR** (Address) or **SPECIFIED**. Choice of using the NAPT address or specifying a different public address to be used for this translation.<br>Public Address Mode**NAPT ADDR** (Address) or **SPECIFIED**. Choice of using the NAPT address or specifying a different public address to be used for this translation.<br>**PROTOCOL** Protocol for this translation.<br>**PUBLIC PORT MODE SPECIFIED** or **ANY PORT**. Choosing **SPECIFIED** brings up the **PUBLIC PORT** and **PUBLIC PORT TYPE** (read-only) settings.<br>**PUBLIC PORT**Numeric Public Port number to be translated (e.g., 23, 80).<br>**PUBLIC PORT TYPE** Read-only port type chosen by the user setting of the **PUBLIC PORT** option.<br>**PRIVATE ADDRESS MODE SPECIFIED** or **ANY INTERNAL**. Choosing **SPECIFIED** brings up the **PRIVATE ADDRESS** option.<br>**PRIVATE PORT MODE SPECIFIED** or **ANY PORT**. Choosing **SPECIFIED** brings up the **PRIVATE PORT** option.<br>**PRIVATE PORT** Numeric Private Port number to be translated to (e.g. 23, 80).<br>**TRANSLATE BODYYES** or **NO**. If set to **YES**, this will translate the body of the data packet and replace the private address with the NAPT address. Default is **NO**, which is used for most applications. |

### Default Gateway Setup

In A.04 TDM code, the default gateway is for the entire unit, not just for the Ethernet Port.

| Default Gateway Setup Instructions | |
|---|---|
| **1** | From the main menu, select **ROUTER**, select **CONFIG**, and select **ROUTES**. |
| **2** | Press Enter on the **DEFAULT GATEWAY** and set the corresponding IP address for the **DEFAULT GATEWAY**. |

# Appendix B. Configuring the Unit for Bridging

## *Initial Setup*

Before the unit can be configured for bridging, DS0s must be mapped. Reference the DS0 Mapping*DS0 Mapping* section in Section 4.2 Appendix A on page 138.

## *Setting up Bridging Options*

If the unit will be used for bridging, continue with the steps below.

## *Bridging*

Bridging is supported by the PPP and Frame Relay protocols. The following procedures describe the bridging configuration for those two protocols.

| **PPP Bridging Setup Instructions** | |
|---|---|
| **1** | From the main menu, select **L2 PROTOCOL (T1[0])>PROTOCOL** and select **PPP**. |
| **2** | Select **CONFIG** and press **<ENTER>**. Then select **MODE** and select **BRIDGE ALL**. |
| **3** | Use the left arrow to return to the main menu; select **BRIDGE**. |
| **4** | The user may confirm that Bridging is activated by selecting **CONFIG** and pressing **<ENTER>**. If the T1[0] interface appears in the list, the Bridging is active on the WAN link. |
| **5** | The time (in minutes) it takes an entry to age out of the Bridge table may be set by down arrowing to **BRIDGE TABLE** and then using the right arrow to select **BRIDGE TABLE AGING**. |

| **Frame Relay Bridging Setup Instructions** | |
|---|---|
| **1** | From the main menu, select **L2 PROTOCOL (T1[0])>PROTOCOL** and select **FRE**. |
| **2** | Select **CONFIG** and press **<ENTER>**. |
| **3** | Set the **MAINTENANCE PROTOCOL TO ANNEX D (ANSI), ANNEX A** (q**933**a)**, LMI**, or **STATIC (NO SIG)**. |
| NOTE | *The* ***MAINTENANCE PROTOCOL*** *should be set based on the Frame Relay switch.* |
| **4** | Select **DLCI MAPPING** and press **<ENTER>**. Then select **MODE** and select **BRIDGE ALL** for all DLCIs which will use bridging. |
| **5** | Use the left arrow to return to the main menu; select **BRIDGE**. |

| Frame Relay Bridging Setup Instructions *(Continued)* | |
|---|---|
| **6** | The user may confirm that Bridging is activated by selecting **CONFIG** and pressing **<ENTER>**. If the T1[0] interface appears in the list, the Bridging is active on the WAN link. |
| **7** | The time (in minutes) it takes an entry to age out of the Bridge table may be set by down arrowing to **BRIDGE TABLE** and then using the right arrow to select **BRIDGE TABLE AGING**. |

## Appendix C. Configuring the Unit for Voice Applications

To set the unit up for voice applications, follow the steps below.

### *Mapping the DS0s*

| DS0 Mapping Instructions | |
|---|---|
| Step | **Action** |
| **1** | From the main menu, select **DS0 MAPS**. |
| **2** | Verify that the **ACTIVE MAP** is set to either **MAP 1** or **MAP 2**. This is the map that is actively running on the unit. The unit has the ability to store two maps.<br>• To edit the current map, press **Enter** on **EDIT/VIEW MAP 1** [+] to view the map. (If Map 1 is the Active Map)<br>• To edit the standby map, press **Enter** on **EDIT/VIEW MAP 2** [+] to view the map. (If Map 2 is the Active Map) |
| NOTE | *The T1 line entering the unit is broken up into 24 DS0s or channels. You must map each voice port you want to use.* |
| **3** | Scroll down to the DS0 that will be mapped. |
| **4** | Set the **SLOT** for the DS0 that you are mapping to **FXS**. |
| **5** | Set the **PORT** of the DS0 that you are mapping. The port number entered must match the voice port the DS0 is being mapped to. **RBS** (robbed bit signaling) will automatically turn on when a port number has been selected. |
| **6** | Map all the DS0s as desired, and exit this menu by pressing the left arrow key. Your changes will save automatically upon exiting the map. |
| **7** | Make sure the **ACTIVE MAP** is set to the map definition you want implemented before exiting the **DS0 MAPS** menu. |

### *Setting up the T1 Interface*

| T1 Interface Setup Instructions | |
|---|---|
| **Step** | **Action** |
| **1** | From the main menu, select **INTERFACES**. |
| **2** | Select **T1[0] CONFIG [+]** and press **ENTER**. |
| **3** | Right arrow to select **FORMAT** and choose **ESF** or **SF**. |

| **T1 Interface Setup Instructions *(Continued)*** | |
|---|---|
| NOTE | *This format must match the format used by the other units in the network.* |
| **4** | Set the **LINE CODE** to **B8ZS** or **AMI**. |
| NOTE | *This line code must match the line code used by the other units in the network.* |
| **5** | Set the **EQUALIZATION** or line build out. The default setting of 0 dB is usually sufficient. |
| **6** | Set the **CSU LPBK** option to **ENABLE, DISABLE,** or **DISABLE ALL** based on whether looping to this unit from another unit will be allowed. |

## *Setting up the FXS Voice Ports*

**FXS Voice Ports Setup Instructions**

| **Step** | **Action** |
|---|---|
| **1** | From the main menu, select **INTERFACES**. |
| **2** | Select **FXS CONFIG [+]** and press **<ENTER>**. |
| **3** | Set the **MODE** of each port to **LOOP START**, **GROUND START**, **TANDEM (E&M), TR08 SINGLE, TR08 UVG**, or **DP0**. |
| NOTE | *This mode needs to be set based on how the network is set up and how each port is being used. Each port does not need to be set to the same mode.*<br>*If the mode is set to* **TANDEM (E&M)**, *be sure to set the* **TANDEM** *options as described in Step 9 and following.* |
| **4** | Set the **TX (dB)** or transmit direction level points of each port. Default is recommended. |
| **5** | Set the **RX (dB)** or receive direction level points of each port. Default is recommended. |
| **6** | Set the **SVC MODE** of each port to either **IN SERVICE** or **OUT OF SVC**. |
| **7** | Set the **LINE Z**, or line impedance, of each port based on the size of the network. Default is recommended. |
| **8** | Set the **MSG IND** to **DISABLE** or **ENABLE**. When set to **ENABLE**, talk path is always open, even in on-hook conditions, in order for FXS message tones to pass through. Disabling this feature will allow higher on-hook voltage but will not allow on-hook messaging other than caller ID. |

| **FXS Voice Ports Setup Instructions** | |
|---|---|
| **9** | Press **Enter** on the **TANDEM [+]** option to view the **TANDEM** options if the port mode is set to **TANDEM (E&M)**. |
| **10** | Set the **CONVERSION MODE** of the port to either **LOOP START** or **GROUND START**. |
| **11** | Set the **SUPERVISION** of the port to either **IMMEDIATE** or **WINK**. |
| NOTE | *Be sure to set the* **TANDEM** *options for each port set to* **TANDEM E&M**. |

# SECTION 4.2 T1 RCU VOICE OVER ATM USER INTERFACE GUIDE

The T1 RCU ATM User Interface Guide is designed for use by network administrators and others who will configure and provision the system. This section provides details unique to the T1 RCU ATM firmware. It contains an overview, application details, configuration information, and menu descriptions. It is recommended that you review Section 4.1, *Commons User Interface Guide* in addition to this section.

## SECTION INDEX

## FIGURES

## TABLES

## 1. T1 RCU MODULE OVERVIEW

The T1 Router Control Unit is a dual board assembly that includes a T1 network interface, DSX-1 PBX interface, Nx56/64 V.35 interface, and built-in IP router. The T1 RCU can provision, test, and provide status for any card in the channel bank. The faceplate has a DB-9 **CRAFT** port connection, dual bantam jack connection, plus network, V.35, and Ethernet LEDs. Six access slots in the Total Access 850 chassis allow the user to combine a variety of voice and data services. Up to six Quad FXS or Quad FXO access modules can be installed to support up to 24 analog voice lines. Other access modules for data applications include the OCU DP and ISDN U-BR1TE. The two remaining access slots support special function cards such as the Echo Canceller Module aVnd the ADPCM compression card.

Used alone, the T1 RCU supports TDM-based applications. Voice over packet/cell applications require that Echo Cancellation techniques be applied to the voice traffic to achieve high quality voice. With the T1 RCU, a separate Echo Canceller Module (*see Echo Canceller without ADPCM (P/N 1203384L1)* on page 20) must be installed in the special slots (A and B) to accommodate these applications. This module cancels echoes for up to 24 voice ports. It is available with and without Adaptive Differential Pulse Code Modulation (ADPCM).

*A separate software load is required to switch from TDM to ATM applications.*

The T1 RCU can operate in two different modes (VoATM or TDM), depending upon the firmware loaded: Channel Bank and Voice over ATM (with the Echo Canceller). Firmware can be updated by using XMODEM transfer protocol via the base unit's **CRAFT** port or by using TFTP from a network server. Refer to DLP-007 and DLP-013 of this manual for instructions on XMODEM upgrade, and refer to DLP-008 for TFTP instructions.

*Only the first two dipswitches on the RCU are used. With the first dip switch up (away from the number, to the right of the unit if you are facing it), the unit boots up in a mode to update the firmware. With the second dip switch up, the unit factory defaults at startup.*

The terminal menu is the access point to all other operations. Each terminal menu item has several functions and submenus that identify and provide access to specific operations and parameters. These menu selections are described later in this User Interface Guide.

## 2. VOICE OVER ATM OVERVIEW

Voice over ATM (VoATM) is the technology used to transmit voice conversations over a data network using Asynchronous Transfer Mode (ATM). There are several potential benefits to moving voice over a data network using ATM. First, the small, fixed-length cells require lower processing overhead. Second, these small, fixed-length cells allow higher transmission speeds than traditional packet switching methods.

ATM allocates bandwidth on demand, making it suitable for high-speed connection of voice, data, and video services. Conventional networks carry data in a synchronous manner. Because empty slots are circulating even when the link is not needed, network capacity is wasted. ATM automatically adjusts the network capacity to meet the system needs.

## 3. VOICE OVER ATM APPLICATION

You can upgrade the T1 RCU for VoATM by adding the Echo Canceller (reference the System Description section, *Echo Canceller without ADPCM (P/N 1203384L1)* on page 20). The Echo Canceller is used in ATM voice applications that require G.168 echo cancellation. The RCU must be using Voice Over ATM firmware to be able to use this module. The module is available with and without ADPCM.

Figure 1 shows a typical VoATM application. The Total Access 850 connects to the ATM Network to provide both voice and high speed data from a single platform.

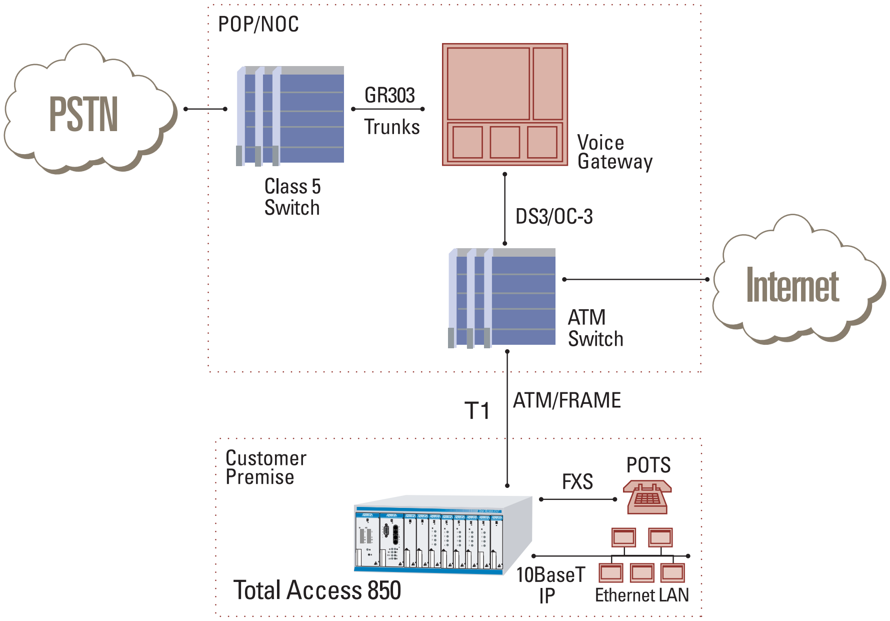


**Figure 1. Voice Over ATM**

NOTE

*Refer to the next section, Configuration, for general configuration instructions.*

*Refer to the appendices at the end of this document for information on using the Total Access 850 in specific applications:*

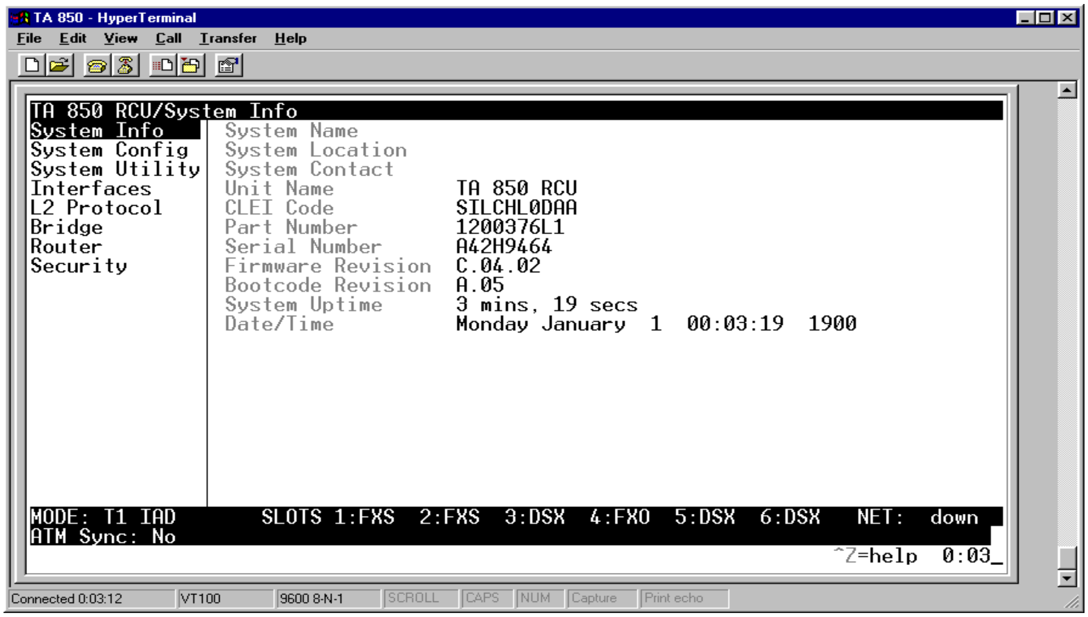
*Appendix A. Voice Gateway Quick Start Procedure (Voice Turn Up) on page 232.*
*Appendix B. RFC1483 Quick Start (IP Routing) on page 236.*

# 4. CONFIGURATION

## SYSTEM INFO

The **SYSTEM INFO** menu provides basic information about the unit as well as data fields for editing information. Figure 2 displays the submenus that are available when you select this menu item.

> *All figures in this section will be representative of the Total Access 850 unit. Firmware revision will reflect C.04.01 for released revisions of software.*



```
TA 850 RCU/System Info
System Info     System Name
System Config   System Location
System Utility  System Contact
Interfaces      Unit Name           TA 850 RCU
L2 Protocol     CLEI Code           SILCHL0DAA
Bridge          Part Number         1200376L1
Router          Serial Number       A42H9464
Security        Firmware Revision   C.04.02
                Bootcode Revision   A.05
                System Uptime       3 mins, 19 secs
                Date/Time           Monday January  1  00:03:19  1900

MODE: T1 IAD        SLOTS 1:FXS  2:FXS  3:DSX  4:FXO  5:DSX  6:DSX   NET:  down
ATM Sync: No
                                                          ^Z=help  0:03_
```

**Figure 2. System Info Menu**

## SYSTEM INFO > SYSTEM NAME

Provides a user-configurable text string for the name of the unit. This name can help you distinguish between different installations. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an underscore). This name will appear on the top line of all screens. The factory default is to have no entry in the system name field.

## SYSTEM INFO > SYSTEM LOCATION

Provides a user-configurable text string for the location of the unit. This field is to help you keep track of the actual physical location of the unit. You can enter up to 31 alphanumeric characters in this field, including spaces and special characters (such as an underscore). The factory default is to have no entry in the system location field.

### SYSTEM INFO > SYSTEM CONTACT

Provides a user-configurable text string for a contact name. You can use this field to enter the name, phone number, or E-mail address of a person responsible for the unit. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an underscore). The factory default is to have no entry in the system contact field

### SYSTEM INFO > UNIT NAME

Product-specific name for the unit.

### SYSTEM INFO > CLEI CODE

The CLEI code for the unit.

### SYSTEM INFO > PART NUMBER

ADTRAN part number for the unit.

### SYSTEM INFO > SERIAL NUMBER

The serial number field will reflect serial number located on bottom of the unit’s chassis.

### SYSTEM INFO > FIRMWARE REVISION

Displays the current firmware revision level of the unit.

### SYSTEM INFO > BOOTCODE REVISION

Displays the bootcode revision.

### SYSTEM INFO > SYSTEM UPTIME

Displays the length of time since the last reboot of the unit.

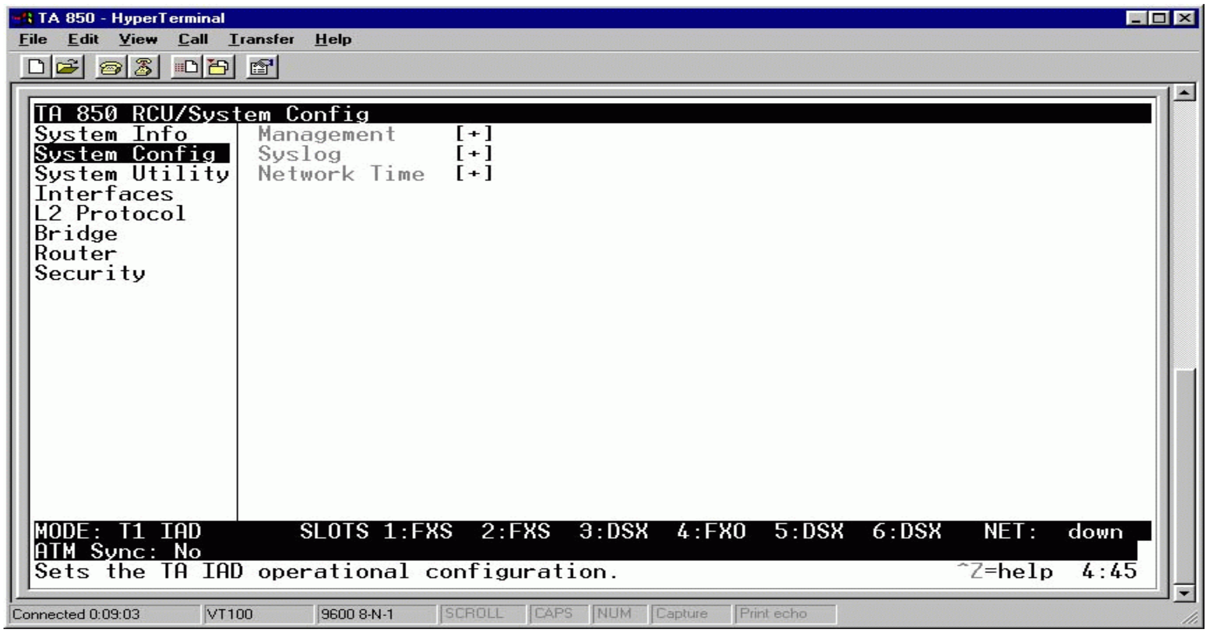
> NOTE *Each time you reset the system, this value resets to 0 days, 0 hours, 0 min. and 0 secs.*

### SYSTEM INFO > DATE/TIME

Displays the current date and time, including seconds. This field can be edited. Enter the time in 24-hour format (such as 23:00:00 for 11:00 pm). Enter the date in mm-dd-yyyy format (for example, 10-30-1998).

## SYSTEM CONFIG

Set up the unit's operational configuration from the **SYSTEM CONFIG** menu. Figure 3 shows the items included in this menu.



```
TA 850 RCU/System Config
System Info      Management     [+]
System Config    Syslog         [+]
System Utility   Network Time   [+]
Interfaces
L2 Protocol
Bridge
Router
Security

MODE: T1 IAD        SLOTS 1:FXS  2:FXS  3:DSX  4:FXO  5:DSX  6:DSX   NET:  down
ATM Sync: No
Sets the TA IAD operational configuration.                      ^Z=help  4:45
```

**Figure 3. System Config Menu**

### SYSTEM CONFIG > MANAGEMENT

Set up the **CRAFT PORT**, **TELNET ACCESS**, **SNMP MANAGEMENT**, and **FDL MANAGEMENT** from this menu.

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT

Set up the **CRAFT PORT** parameters from this menu.

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > PASSWORD PROTECT

The unit's VT 100 **CRAFT** port can be accessed via an RJ 48 connector located on the rear of the unit, or the DB9 connector on the front of the unit.

When **PASSWORD PROTECT** is set to **NO**, the **CRAFT** port is not password protected. When **YES** (def), the unit will prompt for a password upon startup.

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > PASSWORD

This is the text string that is used for comparison when password protecting the **CRAFT** port. By default, no password is entered. You can enter up to 30 characters in this field. Table 1 provides instructions for changing the password.

*The security level for the* **CRAFT** *port is always set to* **FULL**. *This gives full access to all menus.*

*Passwords are case-sensitive and can contain up to 30 alphanumeric characters (including spaces and special characters).*

**Table 1. Instructions for Changing Passwords**

| Step | Action |
|---|---|
| 1 | Select the **PASSWORD** field—a new **PASSWORD** field displays. |
| 2 | Type the new password in the **ENTER** field. |
| 3 | Type the new password again in the **CONFIRM** field. |

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT >IDLE TIME

This option defines the amount of time in minutes user may stay connected without any activity on the **CRAFT PORT** before the user is automatically logged out of the system. A value of **0** disables this inactivity timer function enabling users to stay connected until manually logged out. The value range is **0** (def) to **255** (min).

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > BAUD RATE

This is the asynchronous rate that the **CRAFT** port will run. The possible values are **300, 1200, 2400, 4800, 9600, 19200, 38400**, **57600,** and **115200**. The default value is **9600**.

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > DATA BITS

This is the asynchronous bit rate that the **CRAFT** port will run. The possible values are **7** or **8** (def) bits.

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > PARITY

This is the asynchronous parity that the **CRAFT** port will run. The possible values are **NONE** (def), **ODD**, or **EVEN**.

### SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > STOP BITS

This is the number of stop bits used for the **CRAFT** port. The possible values are **1** (def), **1.5** or **2**.

## System Config > Management > Telnet Access

Activate the Telnet access and set up the various telnet parameters from this menu.

> *The ATM C.01.XX firmware supports one telnet session active at a time. The TDM A.03.XX firmware supports one telnet session active at a time. The TDM A.04 firmware supports five simultaneous telnet sessions.*

## System Config > Management > Telnet Access > Access

Sets **Access** to **On** or **Off.** The factory default value for this parameter is **On**.

## System Config > Management > Telnet Access > Authen Method

Set up the telnet authentication method from this menu. The choices are **Password**, **Radius**, **Password/Radius**, and **Radius/Password**. **Password/Radius** indicates that the unit will try Password Authentication first and if that fails, it will try Radius Authentication. **Radius/Password** indicates that the unit will try Radius authentication first and if that fails, it will try Password authentication. The default is **Password**.

## System Config > Management > Telnet Access > User List

Add telnet users and control the telnet access conditions through this menu.

### #

Display the index number of the telnet users. Up to four users can be configured for access to the unit. Each user can be assigned a security level and idle time.

### Name

The name is a text string of the user name for this session. You can enter up to 15 characters in this field. The factory default is no entry in the **Name** field.

### Password

When the authenticating method is password, or password radius, this text string is used for the password. You can enter up to 30 characters in this field. The factory default is no entry in this field.

### Idle Time (mins)

This sets the amount of time in minutes you can be idle before you are automatically logged off. The factory default is **10 minutes**. The range is 1-255 minutes.

### Level

This is the security level granted to the user. Table 2 gives a brief description of each level. The factory default is **Full**.

**Table 2. Telnet Security Levels**

| Security Level | Description |
|---|---|
| Full | The user has all access to view and configure all menus (same as logging in to the **CRAFT** port) |
| Support | The user has read only access to view the **SYSTEM INFO** menu. The user has privileges to view and change everything under the **SYSTEM CONFIG** menu except for the **CRAFT** port settings, telnet access lists, and the SNMP management communities. The user has full access to the **SYSTEM UTILITY** menu, including the ability to upgrade firmware and reset the unit. The user has full access to the **INTERFACES, L2 PROTOCOL, BRIDGE, ROUTER,** and **DS0** menus. The user does not have the ability to set **RADIUS SERVER** settings under the **SECURITY** menu. |
| Config | The same privileges as support, except that the user does not have privileges to download firmware or configuration from the **SYSTEM UTILITY** menu. The user additionally does not have the privilege to reset the unit remotely, or enter the terminal menu. |
| Router | The user has read only privileges for the **SYSTEM INFO** menu. There is no access to the **SYSTEM CONFIG** menu. The user has **PING** and **TRACEROUTE** access from the **SYSTEM UTILITY** menu. The user is limited to ethernet configuration and status from the **INTERFACES** menu. The user has full access to the **BRIDGE** and **ROUTER** menus. Access is limited to filters only from the **SECURITY** menu. |
| Voice | The user has read only privileges for the **SYSTEM INFO** menu. The user has access to the **PING** and **TRACEROUTE** utilities from the **SYSTEM UTILITIES** menu. The user has full access to the FXS module from the **INTERFACES** menu. |
| Status | The user has read access of all menus except for the following: **SYSTEM CONFIG/CRAFT PORT, SYSTEM CONFIG/TELNET ACCESS, SYSTEM CONFIG/SNMP MANAGEMENT,** and **SECURITY/ RADIUS SERVER**. The user does not have access to **UPGRADE FIRMWARE, UPGRADE CONFIG, PING,** or **TRACEROUTE** menus. The user cannot reset the unit or enter terminal mode. |

## SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > IP ACCESS LIST

Set up the list of allowed telnet managers.

### NETWORK ADDRESS AND MASK

Enter a network address and subnet mask from which telnet access to the unit is allowed. When a remote unit requests telnet access to the unit, if the access list is empty or the remote's IP address matches a list entry, remote access is granted. A subnet mask of 0.0.0.0 will allow any host telnet access, regardless of the network address. A network address of 0.0.0.0 with corresponding netmask 255.255.255.255 will not allow any host telnet access.

The factory default is **0.0.0.0.** for both parameters, which will allow all users telnet IP access.

### SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT

Access the SNMP management and configure the SNMP communities and traps from this menu.

### SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT > ACCESS

When set to **OFF**, SNMP access is denied. When set to **ON**, the unit will respond to SNMP managers based on the configuration. The factory default is **ON**.

### SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT >TRAP DELAY

Time in seconds that represents the delay inserted between the trap creation and trap transmission. The range is 0 to 600 seconds. The factory default is **0 SEC**.

### SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT > COMMUNITIES

Set up the SNMP communities parameters from this menu.

**#**

Displays the index number of the SNMP Communities.
This list is used to set up to 8 SNMP communities that the unit will allow.

**NAME**

This is the text string used to identify the SNMP community. The factory default is no entry in the name parameter.

**PRIVILEGE**

The access for this manager can be assigned three levels. The factory default is **NONE**.

| | |
|---|---|
| **NONE** | No access is allowed for this community or manager. |
| **GET** | Manager can only read items. |
| **GET/SET** | Manager can read and set items. |

**MANAGER IP**

This may be used in conjunction with the Netmask field to define a range of manager IPs. A netmask of 255.255.255.255 defines a single IP as the manager host IP. The default value is **0.0.0.0**.

**NETMASK**

The mask is used to determine which bits of the **MANAGER IP** are significant. A "0" bit means "don't care." A "1" bit means that the corresponding address bits in the incoming SNMP packet must match the address bit in the defined **MANAGER IP**. The netmask of 255.255.255.255 defines a single IP as the manager host IP. The default value is **0.0.0.0**.

### SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT > TRAPS

Sets up the trap manager name and IP from this menu.

**#**

Displays the index number in the SNMP traps table.
This list allows up to 20 managers to be listed to receive traps.

**MANAGER NAME** is the text string describing the name of the entry. It is intended for easy reference and has no bearing on the SNMP trap function. You can enter up to 31 characters in this field. The factory default is no entry in the manager name field.

**MANAGER IP**

This is the IP address of the manager that is to receive the traps. The factory default is **0.0.0.0**.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT

Enables the FDL management and configures mode and IP addresses from this menu.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > MODE

This enables the FDL (only in ESF mode) to be used for management. Learning mode can also be enabled so the unit can "learn" its IP configuration to be used for its FDL management. Once it learns this information from, for example a Total Access 4303, the configuration items populate. The factory default is **ON**.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > LINK IP ADDRESS

This is the local IP address used for FDL management. The FDL uses a separate IP network for communication, distinct from the customer data that is configured under the **ROUTER** menus. The factory default is **0.0.0.0**.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > IP NETMASK

This is the subnet mask defining the IP network used for FDL management. The factory default is **0.0.0.0**.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > FAR-END IP ADDRESS

This is the far-end IP address used for the FDL management. The FDL is a separate IP network from the customer data that is configured under the **ROUTER** menus. The factory default is **0.0.0.0**.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > LEARN ADDRESS

When set to **ON**, the destination address on each received packet is assumed to be the FDL interface address. A 255.255.255.252 netmask is used, which determines the far-side address as well (since there can be only two addresses on a subnet with that netmask). When set to **OFF,** the user must input the IP address assigned to the FDL interface. Default is **ON**.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > ACCEPT ALL SNMP

When set to **ON**, SNMP gets/sets received over the FDL link are always accepted regardless of the community table. When set to **OFF,** the community table is searched for valid manager IP addresses and the SNMP traffic is rejected if a match is not found. Default is **ON**.

### SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > MTU

Maximum Transmit Unit allows the user to set the largest acceptable IP packets that will be transmitted before configuration takes place. The range is 64 to 256 kbps. The default is **256 KBPS**.

### SYSTEM CONFIG > SYSLOG

Configure the unit Syslog client for use with a Syslog server (supplied with ADTRAN Utilities or available on most Unix platforms) from this menu.

NOTE *For additional information, reference RFC3164: The BSD Syslog Protocol.*

### SYSTEM CONFIG > SYSLOG > SYSLOG IP

IP address of the syslog daemon to which log message should be sent. The values must be dotted decimal notation.

### SYSTEM CONFIG > SYSLOG > SYSLOG FORMAT

The **SYSLOG FORMAT** is the format of log messages. "**ADTRAN**" uses a format that is compatible with Adtran Utilities and forces the Syslog Facility to LOCAL0. **UNIX** uses the traditional Unix format and reports at the configured facility level.

NOTE *Adtran Utilities may malfunction if messages are received in the Unix format.*

### SYSTEM CONFIG > SYSLOG > SYSLOG FACILITY

The choices are: **LOCAL0**, **LOCAL1**, **LOCAL2**, **LOCAL3**, **LOCAL4**, **LOCAL5**, **LOCAL6**, **LOCAL7**. **SYSLOG FACILITY** is the facility level for all messages forwarded from the unit to the syslog server. This allows all messages received from the IAD to be filtered by facility level. See *RFC3164: The BSD Syslog Protocol*..

NOTE *This does not have to correspond to the facility level shown in the terminal mode option. See SYSLOG Facility using Terminal Mode on page 162.*

The remaining Syslog parameters have the following level choices:

FATAL (Highest priority)
ALERT
CRITICAL
ERROR
WARNING
NOTICE
INFO
DEBUG (Lowest priority)

Every log message generated by the IAD has a reporting level priority. If the message priority is lower than the configured priority for the destination log, the message is not forwarded to the syslog daemon. See *RFC3164: The BSD Syslog Protocol*. The lower the log level, the more messages that will be generated. Setting reporting levels to DEBUG may negatively affect the performance of the IAD, including causing the IAD to reset.

> NOTE *ADTRAN recommends using DEBUG for only short periods of time for debug purposes only.*

### *SYSLOG using Terminal Mode*

Another option for configuring syslog is using the terminal mode command **log dump <logname>**. The logname must be all CAPS and be one of the following names:

FATAL
ALERT
CRITICAL
ERROR
WARNING
NOTICE
INFO
DEBUG

The command will dump all messages for the indicated log (**ALL LEVEL** shows all log messages) stored in the internal log buffer to the command line display.

### SYSTEM CONFIG > SYSLOG > ALL LEVEL

This entry allows setting the default reporting level for all log entries. If **ALL LEVEL** is a lower priority than the individual log entry level, **ALL LEVEL** overrides the individual log reporting level.

### SYSTEM CONFIG > SYSLOG > KERNEL LEVEL

Minimum required level for sending KERNEL log messages.

### SYSTEM CONFIG > SYSLOG > DHCP LEVEL

Minimum required level for sending DHCP log messages.

### SYSTEM CONFIG > SYSLOG > NTP LEVEL

Minimum required level for sending NTP log messages.

### SYSTEM CONFIG > SYSLOG > TFTP LEVEL

Minimum required level for sending TFTP log messages.

### SYSTEM CONFIG > SYSLOG > TELNET LEVEL

Minimum required level for sending TELNET log messages.

### SYSTEM CONFIG > SYSLOG > IP LEVEL

Minimum required level for sending IP log messages.

### SYSTEM CONFIG > SYSLOG > PPP LEVEL

Minimum required level for sending PPP log messages.

### SYSTEM CONFIG > SYSLOG > NAT LEVEL

Minimum required level for sending NAT log messages.

### SYSTEM CONFIG > SYSLOG > ARP LEVEL

Minimum required level for sending ARP log messages.

### SYSTEM CONFIG > SYSLOG > UDP LEVEL

Minimum required level for sending UDP log messages.

### SYSTEM CONFIG > SYSLOG > NETWRITE LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG > TCP LEVEL

Minimum required level for sending TCP log messages.

### SYSTEM CONFIG > SYSLOG > COMPSYS LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG > CONSOLE LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG > CFGXFER LEVEL

Minimum required level for sending configuration transfer log messages.

### SYSTEM CONFIG > SYSLOG > ROUTER LEVEL

Minimum required level for sending router log messages.

### SYSTEM CONFIG > SYSLOG > NONVOL LEVEL

Minimum required level for sending nonvolatile memory log messages.

### SYSTEM CONFIG > SYSLOG > NOKIA LEVEL

Minimum required level for sending log messages about communication with the Nokia DSLAM. Messages are only generated for products with an SDSL WAN interface.

### SYSTEM CONFIG > SYSLOG > AUTOBAUD LEVEL

Minimum required level for sending log messages about communication with the Lucent Stinger DSLAM. Messages are only generated for products with an SDSL WAN interface.

### SYSTEM CONFIG > SYSLOG > TOLLBRG LEVEL

Minimum required level for sending log messages about communication with the Tollbridge Voice Gateway. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > CMCP LEVEL

Minimum required level for sending log messages about communication with the CopperMountain DSLAM. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > SDSL LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG > L1 LEVEL

Minimum required level for sending log messages about WAN physical or Layer 1 connection.

### SYSTEM CONFIG > SYSLOG > ETH LEVEL

Minimum required level for sending log messages about Ethernet physical connection.

### SYSTEM CONFIG > SYSLOG > ICMP LEVEL

Minimum required level for sending ICMP log messages.

### SYSTEM CONFIG > SYSLOG > CONFIG LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG >DS0 LEVEL

Minimum required level for sending log messages about DSO mapping.

### SYSTEM CONFIG > SYSLOG > SELFTEST LEVEL

Minimum required level for sending log messages about selftest.

### SYSTEM CONFIG > SYSLOG > VOICE LEVEL

Minimum required level for sending log messages about AAL2 voices services.
Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > JETSTREAM LEVEL

Minimum required level for sending log messages about communication with the JetStream Voice Gateway. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > POTS LEVEL

Minimum required level for sending log messages about POTS line cards and services.

### SYSTEM CONFIG > SYSLOG > LESCAS LEVEL

Minimum required level for sending messages about communication with LESCAS compatible Voice Gateways. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > ATM LEVEL

Minimum required level for sending ATM log messages. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > COPPERCOM LEVEL

Minimum required level for sending log messages about communication with the CopperCom Voice Gateway. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > VOFR LEVEL

Minimum required level for sending voice-over-frame-relay log messages about communication with the CopperMountain DSLAM. Messages are only generated for ATM products.

### SYSTEM CONFIG > SYSLOG > XMODEM LEVEL

Minimum required level for sending XMODEM log messages for firmware and configuration transfers.

### SYSTEM CONFIG > SYSLOG > EMWEB LEVEL

This parameter is for ADTRAN internal use only.

### SYSTEM CONFIG > SYSLOG > FRELAY LEVEL

Minimum required level for sending frame relay log messages.

### SYSTEM CONFIG > SYSLOG > BRIDGE LEVEL

Minimum required level for sending bridge mode log messages.

### SYSTEM CONFIG > SYSLOG > MAINT LEVEL

Minimum required level for sending **CRAFT** port log messages.

### SYSTEM CONFIG > SYSLOG > HDLC LEVEL

Minimum required level for sending low level HDLC log messages.

### SYSTEM CONFIG > SYSLOG > VOATM LEVEL

Minimum required level for sending Voice-over-ATM log messages.

### SYSTEM CONFIG > SYSLOG > PPPOA LEVEL

Minimum required level for sending PPP-over-ATM log messages.

### SYSTEM CONFIG > SYSLOG > FDL LEVEL

Minimum required level for sending FDL log messages.

### SYSTEM CONFIG > NETWORK TIME

Activate the network time and configure the server type, time zone and various other network time parameters from this menu.

### SYSTEM CONFIG > NETWORK TIME > SERVER TYPE

The unit time can be entered manually from the **SYSTEM INFO** menu, or the unit can receive time from an NTP/SNTP server. The **NETWORK TIME** menu includes all parameters relating to how the unit communicates with the time server.

The server type defines the port on which the unit will listen to receive timing information from the time server. The choices are **NT TIME** and **SNTP**. When set to **NT TIME**, the unit will receive time from an NT server running SNTP software on its TIME port. When set to **SNTP**, the unit will receive time directly from an SNTP server. The factory default is **SNTP**.

### SYSTEM CONFIG > NETWORK TIME > ACTIVE

This network timing feature can be turned on and off. It determines whether the unit will request and receive time from a time server. The factory default is **NO**.

### SYSTEM CONFIG > NETWORK TIME > TIME ZONE

All time zones are based off of Greenwich Mean Time (GMT). The choices are listed below

- **GMT**
- **GMT -5 (EASTERN)**
- **GMT -6 (CENTRAL)**
- **GMT -7 (MOUNTAIN)**
- **GMT -8 (PACIFIC)**
- **GMT -9 (ALASKA)**
- **GMT -10 (HAWAII)**

The factory default is **GMT-6 (CENTRAL)**.

### SYSTEM CONFIG > NETWORK TIME > ADJUST FOR DAYLIGHT SAVING

Since some areas of the world use Daylight Savings Time, the unit is designed to adjust the time on the first Sunday in April and the last Sunday in October accordingly if this option is turned on. The factory default is **YES**.

### SYSTEM CONFIG > NETWORK TIME > HOST ADDRESS

This is the IP address of the time server that the unit will request and receive time from. The factory default is no entry in the host address field.

### SYSTEM CONFIG > NETWORK TIME > REFRESH

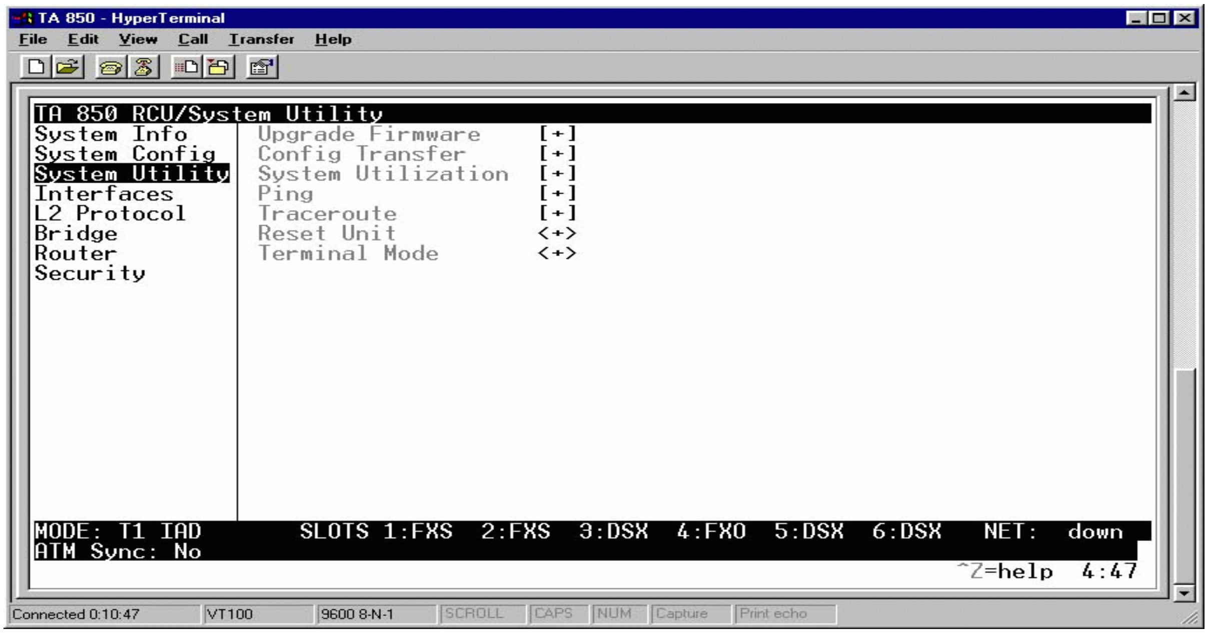
This is the interval of time between each request the unit sends out to the time server. A smaller refresh time guarantees that the unit receives the correct time from the server and corrects possible errors more quickly. This may be more taxing on the machine. A range of refresh times is available for the user to decide which is best for their unit. Choices include **5 MINS, 10 MINS, 15 MINS, 20 MINS, 25 MINS, 30 MINS, 35 MINS, 40 MINS, 45 MINS, 50 MINS, 55 MINS,** and **60 MINS**. The factory default is **60 MINS**.

### SYSTEM CONFIG > NETWORK TIME > STATUS

This displays the current status of the time negotiation process. If an error is displayed, check all connections and configurations to try to resolve the problem.

## SYSTEM UTILITY

Use the **SYSTEM UTILITY** menu to view and set the system parameters shown in Figure 4.



```
TA 850 RCU/System Utility
System Info      Upgrade Firmware     [+]
System Config    Config Transfer      [+]
System Utility   System Utilization   [+]
Interfaces       Ping                 [+]
L2 Protocol      Traceroute           [+]
Bridge           Reset Unit           <+>
Router           Terminal Mode        <+>
Security

MODE: T1 IAD        SLOTS 1:FXS  2:FXS  3:DSX  4:FXO  5:DSX  6:DSX   NET:  down
ATM Sync: No
                                                             ^Z=help  4:47
```

**Figure 4. System Utility Menu**

### SYSTEM UTILITY > UPGRADE FIRMWARE

Select the firmware upgrade method and perform upgrade from this menu.

### SYSTEM UTILITY > UPGRADE FIRMWARE > TRANSFER METHOD

The customer can update firmware when unit enhancements are released.

The two methods for upgrading are **XMODEM** and **TFTP**. (See the DLP section of this manual for more information.) **TFTP** requires a TFTP server running on the network. The unit starts a TFTP client function which gets the upgrade code from the TFTP server. Selecting **XMODEM** will load the upgrade code through the **CRAFT** port using any PC terminal emulator with XMODEM capability. The factory default is **TFTP**.

### SYSTEM UTILITY > UPGRADE FIRMWARE > TFTP SERVER ADDRESS

This is required when the transfer method is TFTP. It is the IP address or domain name (if DNS is configured) of the TFTP server. The factory default is no entry in the **TFTP SERVER ADDRESS** field.

### SYSTEM UTILITY > UPGRADE FIRMWARE > TFTP SERVER FILENAME

This is required when the transfer method is TFTP. It is the case-sensitive file name which contains the upgrade code. The factory default is no entry in the **TFTP SERVER FILENAME** field.

### SYSTEM UTILITY > UPGRADE FIRMWARE > TRANSFER STATUS

This appears when TFTP is used. It displays the status of the transfer as it happens. Any error or success message will be displayed here.

### SYSTEM UTILITY > UPGRADE FIRMWARE > START TRANSFER

This activator is used when the configurable items in this menu are complete. This will initiate the transfer for either TFTP or XMODEM upgrades.

> NOTE
>
> *Before using **START TRANSFER**, the unit should have a valid IP address, subnet mask, and default gateway (if required). See DLP-002, Setting IP Parameters for the Total Access 850 for more information.*

### SYSTEM UTILITY > UPGRADE FIRMWARE > ABORT TRANSFER

Use this activator to cancel any TFTP transfer in progress.

### SYSTEM UTILITY > CONFIG TRANSFER

Select the config transfer method and perform the transfer from this menu.

### SYSTEM UTILITY > CONFIG TRANSFER > TRANSFER METHOD

Sends a file containing the unit configuration to a PC connected to the **CRAFT** port using XMODEM protocol or to a file on a TFTP server using the TFTP protocol.

**CONFIG TRANSFER** also lets you save the unit configuration as a backup file, so you can use the same configuration with multiple units. In addition, **CONFIG TRANSFER** can retrieve a configuration file from a TFTP server.

To support these transfers, ADTRAN delivers a TFTP program with the unit called TFTP Server. You can configure any PC running Microsoft Windows with this software, and store a configuration file.

> NOTE
>
> *Before using **START TRANSFER**, the unit should have a valid IP address, subnet mask, and default gateway (if required). See DLP-002, Setting IP Parameters for the Total Access 850 for more information.*

Only one configuration transfer session (upload or download) can be active at a time. **XMODEM** and **TFTP** are supported.

### System Utility > Config Transfer > TFTP Server IP Address

Specifies the IP address of the TFTP server. Get this number from your system administrator. If using the ADTRAN Utilities TFTP server, this number appears in the TFTP server status window. The factory default value is **0.0.0.0**.

### System Utility > Config Transfer > TFTP Server Filename

Defines the name of the configuration file that you transfer to or retrieve from the TFTP server. The default name is **ta_iad.cfg**, but you can edit this name.

### System Utility > Config Transfer > Current Transfer Status

Indicates the current status of the update.

### System Utility > Config Transfer > Previous Transfer Status

Indicates the status of the previous update.

### System Utility > Config Transfer > Load And Use Config

Retrieves the configuration file specified in the **TFTP Server Filename** field from the server. To start this command, enter **Y** to begin or enter **N** to cancel.

CAUTION

*If you execute this command, the unit retrieves the configuration file, reboots, then restarts using the new configuration.*

### System Utility > Config Transfer > Save Config Remotely

Saves the configuration file specified in **TFTP Server Filename** to the server identified in **TFTP Server IP Address**. To start this command, enter **Y** to begin or enter **N** to cancel.

CAUTION

*Before using this command, you must have identified a valid TFTP server in* ***TFTP Server IP Address****.*

### System Utility > System Utilization

View the CPU utilization stats from this menu.

### System Utility > System Utilization > Performance

Clear the system utilization stats and view the total and current CPU utilization stats from this menu.

### System Utility > System Utilization > Performance > Total Avg CPU Utilization

**Total Avg CPU Utilization** is a running total of CPU utilization since the last reset.

### SYSTEM UTILITY > SYSTEM UTILIZATION > PERFORMANCE > CURRENT AVG CPU UTILIZATION

**CURRENT AVG CPU UTILIZATION** is the running total of CPU utilization since the last clear.

### SYSTEM UTILITY > SYSTEM UTILIZATION > PERFORMANCE >TOTAL AVG ISR UTILIZATION

The Total Avg ISR Utilization is a running total average of the ISR Utilization.

### SYSTEM UTILITY > SYSTEM UTILIZATION > PERFORMANCE > CLEAR STATS

This activator will clear all the system utilization performance stats.

### SYSTEM UTILITY > PING

Activate the ping test and define the ping packet characteristics from this menu.

### SYSTEM UTILITY > PING > START/STOP

Activator to start and cancel a ping test.

NOTE *Only one ping session can be active at a time.*

NOTE *Diagnostic features such as ping, extended ping, traceroute, extended traceroute, and telnet client can also be performed via* **TERMINAL MODE** *(see page 173).*

### SYSTEM UTILITY > PING > HOST ADDRESS

IP address or domain name (if DNS is configured) of device to receive the ping. The factory default is no entry in the host address field.

### SYSTEM UTILITY > PING > SIZE (40-1500)

Total size of the ping to send. Range is **40** to **1500** bytes. The default is **64**.

### SYSTEM UTILITY > PING > # OF PACKETS

Total packets to send every 2 seconds. Setting this to **0** allows the client to ping continuously. The default is **5**.

### SYSTEM UTILITY > PING > # TRANSMITS

Total packets sent (read only).

### SYSTEM UTILITY > PING > # RECEIVES

Total packets received (read only).

### SYSTEM UTILITY > PING > % LOSS

Percentage loss based on ping returned from host (read only).

### SYSTEM UTILITY > TRACEROUTE

Utility program used to trace a data path to a final destination.

### SYSTEM UTILITY > TRACEROUTE > TRACE TARGET

Specifies the IP address of the remote system to trace the routes to.

### SYSTEM UTILITY > TRACEROUTE > MAXIMUM HOPS

Specifies the maximum number of router exchanges allowed when traveling to the final destination (specified using the **TRACE TARGET** field) Range is **1** to **30**. Default is **30**.

### SYSTEM UTILITY > TRACEROUTE > TIMEOUT (IN SECS)

Specifies the maximum delay (in milliseconds) given to a host (along a path to the final destination) to respond to the probe datagram sent before considering the packet a failure.

### SYSTEM UTILITY > TRACEROUTE > RETRIES

Specifies the number of times the probe datagram is sent to each host (along the path to the final destination).

### SYSTEM UTILITY > TRACEROUTE > BEGIN TRACEROUTE

Activates the traceroute process by sending a probe datagram with a Time To Live (TTL) value of 1.

### SYSTEM UTILITY > RESET UNIT

Selecting this activator will power reset the unit.

### SYSTEM UTILITY > TERMINAL MODE

Selecting the terminal mode gives the user a command-line prompt to perform utilities such as pings, traceroutes, resets, firmware updates, configuration, and more. **TERMINAL MODE** can also be accessed by using the shortcut keys **CNTRL** T from other menu screens. From this command-line prompt, you can:

- Perform a reset with the command "reset"
- Perform a factory restore with the command "factory_reset"
- Configure the unit. The unit has the ability to download a text file which contains the configuration of the entire unit. This configuration may then be altered in a text editor, and then uploaded to a unit. (See DLP-013, *A.03 to A.04 Firmware Upgrade* for further assistance.)
- Debug and troubleshoot. This function would be carried out with the assistance of ADTRAN Technical Support.
- Start and stop the fail-safe timer for the auto-config feature.
- Perform a firmware upgrade via TFTP.

  **upgrade_firmware *hostname filename***
- Use the **save** command to write the entire configuration to flash.
- Display the unit's MAC address with the command **mac**
- Perform a ping or extended ping. Syntax is:

  **ping hostname/address [repeat xx] [size xx] [timeout xx] [source xx] [noNat]**

  Options:

| | |
|---|---|
| repeat <repeat count> | Number of pings to send (default 5) |
| size (datagram size) | Range is 40-1500 |
| timeout (seconds) | Timeout in seconds (range 1-10) |
| source (address or name) | Source address or interface name to use |
| noNat | Do not NAT the ping packet |

Options may be entered in any order and may be truncated.
Valid interface names are eth0, fdl0, ppp0, fr0, fr1, etc.

Example usage: **ping 10.0.0.5 r si 1500 so eth0 n**
This will ping with a repeat count of 10. The datagram size is 1500 bytes, and the source address used in the ping packet will be the ethernet IP address. The “noNat” option has been specified, so if NAT is enabled, this packet will NOT be translated.

- Perform a traceroute or extended traceroute. Syntax is:

  **traceroute hostname/address [hops xx] [timeout xx] [retries xx] [source xx] [noNat]**

  Options:

  | | |
  |---|---|
  | hops <hops count> | Max number of hops (default 30) |
  | timeout <seconds> | Timeout in seconds (default 3) |
  | retries <seconds> | Number of retries per hop (default 3) |
  | source <address or name> | Source address or interface name to use |
  | noNat | Do not NAT the trace packets |

  Options may be entered in any order and may be truncated.
  Valid interface names are eth0, fdl0, ppp0, fr0, fr1, etc.

  Example usage: **trace 10.0.0.5 h 20 t 1 r 1 so eth0**
  This will perform a trace to 10.0.0.5 with a max hop count of 20. The timeout for each hop is 1 second, and the retry count per hop is 1. The ethernet IP will be used as the source address, and the packet WILL go through NAT if NAT is enabled, meaning that the packet will be translated and the source address will be replaced by the NAPT address.

- Use the telnet client feature to telnet to a remote host. Syntax is:

  **telnet hostname/address [port xx]**

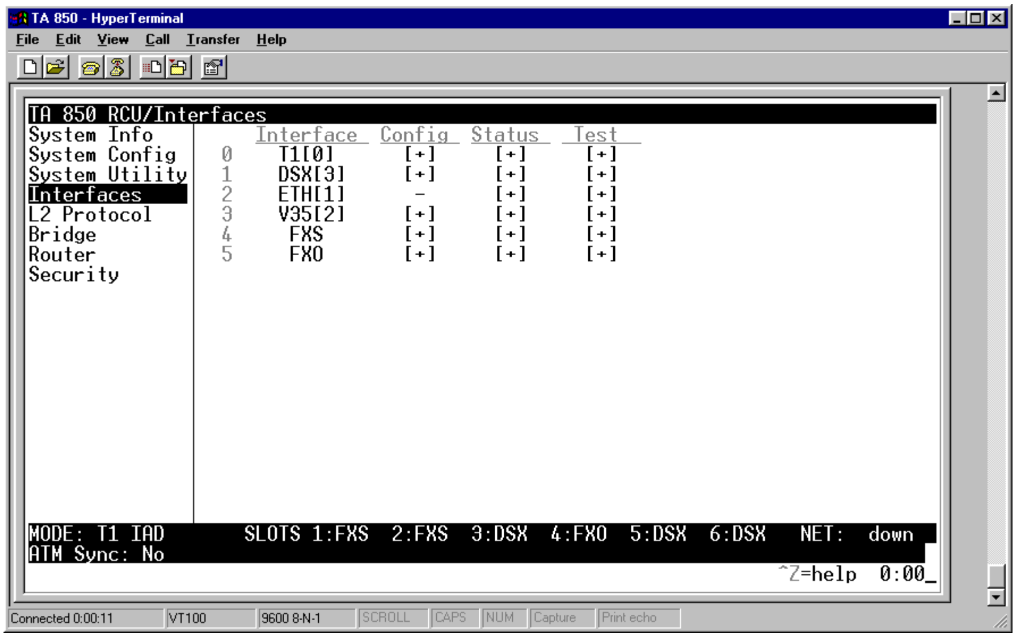
  Default port is 23 (TELNET).

- To exit terminal mode, type **exit** or **!exit**,
  **exit -** if any configuration have been made, you will be prompted whether or not to save these changes. If no changes were made then the terminal session will exit without the confirm message.
  **!exit -** exit without saving or applying any configuration changes.

> NOTE *Extended ping, extended traceroute, and telnet client are new features initially available in C.04.02. These functions may be performed simultaneously from multiple user sessions.*

## INTERFACES

Use the **INTERFACES** menu to view and configure parameters for the **T1**, **ETHERNET**, **V.35**, and **FXS** interfaces as shown in Figure 5.



```
TA 850 RCU/Interfaces
System Info        Interface  Config  Status   Test
System Config   0    T1[0]     [+]     [+]     [+]
System Utility  1    DSX[3]    [+]     [+]     [+]
Interfaces      2    ETH[1]     -      [+]     [+]
L2 Protocol     3    V35[2]    [+]     [+]     [+]
Bridge          4     FXS      [+]     [+]     [+]
Router          5     FXO      [+]     [+]     [+]
Security

MODE: T1 IAD        SLOTS 1:FXS  2:FXS  3:DSX  4:FXO  5:DSX  6:DSX   NET:  down
ATM Sync: No
                                                               ^Z=help  0:00_
```

**Figure 5. Interfaces Menus**

## INTERFACES (T1[0])

View the T1 interface status and configure T1 parameters from this menu.

NOTE *The 0 in T1[0] represents a physical port. The T1 physical port is always 0.*

### INTERFACES (T1[0]) > CONFIG

Configure the various T1 parameters and enable/disable loopbacks from this menu.

### INTERFACES (T1[0]) > CONFIG > TIMING MODE

Choices are **NETWORK** and **INTERNAL**. Select **NETWORK** when the unit will receive timing from the network. Select **INTERNAL** when the unit will generate the timing. Default is **NETWORK**.

### Interfaces (T1[0]) > Config > Format

This sets the frame format for the T1 interface. The setting must match the frame format of the circuit to which the interface is connected. Choices are **ESF** or **SF**. Extended Superframe (**ESF**) provides a non-disruptive means of full-time monitoring on the facility datalink (FDL). Default is **ESF**.

> **SF** *is equivalent to the D4 frame format.*

### Interfaces (T1[0]) > Config > Line Code

This sets the line code for the T1 interface. The setting must match the line code of the circuit to which the interface is connected. Choices are **B8ZS** (bipolar with 8-zero substitution) and **AMI** (alternate mark inversion). Default is **B8ZS**.

### Interfaces (T1[0]) > Config > Equalization

Select the line build out for the T1 interface. These are attenuation settings. 0 dB is the strongest signal and the other settings make the T1 transmit signal weaker. The setting of this field depends on whether the circuit is provisioned for DS1 by the telephone company. The choices are **0 dB**, **-7.5 dB**, **-15 dB**, **-22 dB**. Default is **0 dB**.

### Interfaces (T1[0]) > Config > CSU Lpbk

Choices are **Enable**, **Disable**, and **Disable All**. Default is **Enable**. This allows the unit to either respond or not respond to CSU loop up commands.

### Interfaces (T1[0]) > Status

Displays the T1 status including performance data and alarm histories.

### Interfaces (T1[0]) > Status > Performance

Displays the T1 performance data.

### Interfaces (T1[0]) > Status > Performance > Time Frame

Choices are **Current**, **15 Min**, and **24 Hr**. Default is **Current**. The performance fields -- either **Current**, **15 Min**, or **24 Hr**. -- provide status on key performance measures as specified in ANSI T1.403 and AT&T TR 54016 for each of the T1 ports. When **Current** is chosen, the performance data for the current 15 minute window is shown.

### Interfaces (T1[0]) > Status > Performance > Clear

Clears information for the selected port. Press <**Enter**> when the cursor is over this field to clear the data.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > ES

**ES** (Errored Second) - For ESF mode, an errored second is defined as a second with one or more Path Code Violations (PCVs), or one or more Out of Frame (OOF) defects, or one or more Controlled Slip events, or a detected AIS (blue alarm) defect.  For D4 (SF) mode, the presence of Bipolar Violations (BPVs) also triggers an errored second.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > SES

**SES** (Severely Errored Second) - For ESF mode, an **SES** is a second with 320 or more PCVs, or one or more OOF defects, or a detected AIS defect.  For D4 (SF) mode, an **SES** is a second with one or more Framing Error events, or an OOF defect, or at least 1544 Line Code Violations or more.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > SEF

**SEF** (Severely Errored Frame) - An **SEF** condition occurs when 2 out of 6 consecutive frame bits are in error.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > FS

**FS** (Frame Slip) - A frame slip is defined as one or more frame bit errors in a one-second interval.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > LCV

**LCV** (Line Code Violation) - A Line Code Violation is defined as a Bipolar Violation (BPV), not including the B8ZS code word if B8ZS is employed.  The number displayed is **LCV** events, which is defined as one or more BPVs in a one-second interval.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > SLP

SLP (Slip Error Event) - This occurs when a received frame is either repeated or deleted.  A **SLP** error indicates a timing problem.

### INTERFACES (T1[0]) > STATUS > PERFORMANCE > UAS

**UAS** (Unavailable Seconds) - When 10 consecutive **SES**s have been logged, the unit is declared in an unavailable state, the 10 **SES**s are cleared, and the Unavailable Seconds count begins to increment starting with 10.  The unavailable state is cleared when 10 consecutive non-SES seconds have occurred.

### INTERFACES (T1[0]) > STATUS > ALARMS

Displays current alarms and alarm history for T1 interface.

### INTERFACES (T1[0]) > STATUS > ALARMS > CURRENT ALARMS

Displays the current alarms on the T1 interface. An asterisk in a field indicates that an alarm is active.

| | |
|---|---|
| LOS | Loss of Signal. No signal detected on port interface. |
| RED | Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF). |
| YELLOW | Remote alarm indicator (RAI) being received on port. |
| BLUE | Receiving unframed all ones from the port; alarm indicator signal (AIS). |

### INTERFACES (T1[0]) > STATUS > ALARMS > ALARM HISTORY

Displays the alarm history for the T1 interface. An asterisk in a field indicates that an alarm has occurred on the T1 interface since the last clear history.

| | |
|---|---|
| LOS | Loss of Signal. No signal detected on port interface. |
| RED | Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF). |
| YELLOW | Remote alarm indicator (RAI) being received on port. |
| BLUE | Receiving unframed all ones from the port; alarm indicator signal (AIS). |

### INTERFACES (T1[0]) > STATUS > ALARMS > CLEAR HISTORY

Selecting this activator will clear the Alarm History for the T1 interface.

### INTERFACES (T1[0]) > STATUS >RX LEVEL

Displays the signal level in decibels of the received T1 signal.

### INTERFACES (T1[0]) > TEST

These options are used to initiate local and remote loopback tests and display the test status.

### INTERFACES (T1[0]) > TEST > LOC LB

Loopback of the local unit. Choices are **NONE**, **LINE**, **AND PAYLOAD**. **LINE** Loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **PAYLOAD** Loopback is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

### Interfaces (T1[0]) > Test > Rem LB

Loopback of remote unit. Choices are **None**, **Line**, and **Payload**. **Line** Loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **Payload** Loopback is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **None** disables the loopback test. Default is **None**.

### Interfaces (T1[0]) > Test > Test Status

Indicates whether a test is in progress.

## Interfaces (DSX[3])

View the DSX1 interface status and configure T1 parameters from this menu.

NOTE *The 3 in DSX[3] represents a physical port. The DSX1 physical port is always 3.*

### Interfaces (DSX[3]) > Config

Configure the various DSX1 parameters and enable/disable loopbacks from this menu.

### Interfaces (DSX[3]) > Config > Format

This sets the frame format for the DSX1 interface. The setting must match the frame format of the circuit to which the interface is connected. Choices are **ESF**, **SF**. Extended Superframe (**ESF**) provides a non-disruptive means of full-time monitoring on the facility datalink (FDL). Default is **ESF**.

NOTE ***SF** is equivalent to the D4 frame format.*

### Interfaces (DSX[3]) > Config > Line Code

This sets the line code for the DSX1 interface. The setting must match the line code of the circuit to which the interface is connected. Choices are **B8ZS** (bipolar with 8-zero substitution) and **AMI** (alternate mark inversion). Default is **B8ZS**.

### Interfaces (DSX[3]) > Config > Equalization

Select the line build out for the DSX1 interface. The choices are **0 dB**, **266 ft, 399 ft, 533 ft, 655 ft, or -7.5 dB**. Default is **0 dB**. The 7.5 dB setting is provided for terminal equipment that has trouble recovering a full 0dB level signal (typically one with a DS1 long haul line interface).

### INTERFACES (DSX[3]) > CONFIG > CSU LPBK

Choices are **ENABLE**, **DISABLE**, and **DISABLE ALL**. Default is **ENABLE**. This allows the unit to either respond or not respond to CSU loop up commands.

### INTERFACES (DSX[3]) > STATUS

Displays the T1 status including performance data and alarm histories.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE

Displays the T1 performance data.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > TIME FRAME

Choices are **CURRENT**, **15 MIN**, and **24 HR**. Default is **CURRENT**. The performance fields -- either **CURRENT**, **15 MIN**, or **24 HR**. -- provide status on key performance measures as specified in ANSI T1.403 and AT&T TR 54016 for each of the T1 ports. When **CURRENT** is chosen, the performance data for the current 15 minute window is shown.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > CLEAR

Clears information for the selected port. Press <**Enter**> when the cursor is over this field to clear the data.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > ES

**ES** (Errored Second) - For ESF mode, an errored second is defined as a second with one or more Path Code Violations (PCVs), or one or more Out of Frame (OOF) defects, or one or more Controlled Slip events, or a detected AIS (blue alarm) defect. For D4 (SF) mode, the presence of Bipolar Violations (BPVs) also triggers an errored second.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > SES

**SES** (Severely Errored Second) - For ESF mode, an **SES** is a second with 320 or more PCVs, or one or more OOF defects, or a detected AIS defect. For D4 (SF) mode, an **SES** is a second with one or more Framing Error events, or an OOF defect, or at least 1544 Line Code Violations or more.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > SEF

**SEF** (Severely Errored Frame) - An **SEF** condition occurs when 2 out of 6 consecutive frame bits are in error.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > FS

**FS** (Frame Slip) - A frame slip is defined as one or more frame bit errors in a one-second interval.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > LCV

**LCV** (Line Code Violation) - A Line Code Violation is defined as a Bipolar Violation (BPV), not including the B8ZS code word if B8ZS is employed. The number displayed is **LCV** events, which is defined as one or more BPVs in a one-second interval.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > SLP

SLP (Slip Error Event) - This occurs when a received frame is either repeated or deleted. A **SLP** error indicates a timing problem.

### INTERFACES (DSX[3]) > STATUS > PERFORMANCE > UAS

**UAS** (Unavailable Seconds) - When 10 consecutive **SES**s have been logged, the unit is declared in an unavailable state, the 10 **SES**s are cleared, and the Unavailable Seconds count begins to increment starting with 10. The unavailable state is cleared when 10 consecutive non-SES seconds have occurred.

### INTERFACES (DSX[3]) > STATUS > ALARMS

Displays current alarms and alarm history for T1 interface.

### INTERFACES (DSX[3]) > STATUS > ALARMS > CURRENT ALARMS

Displays the current alarms on the T1 interface. An asterisk in a field indicates that an alarm is active.

| | |
|---|---|
| LOS | Loss of Signal. No signal detected on port interface. |
| RED | Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF). |
| YELLOW | Remote alarm indicator (RAI) being received on port. |
| BLUE | Receiving unframed all ones from the port; alarm indicator signal (AIS). |

### INTERFACES (DSX[3]) > STATUS > ALARMS > ALARM HISTORY

Displays the alarm history for the T1 interface. An asterisk in a field indicates that an alarm has occurred on the T1 interface since the last clear history.

| | |
|---|---|
| LOS | Loss of Signal. No signal detected on port interface. |
| RED | Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF). |
| YELLOW | Remote alarm indicator (RAI) being received on port. |
| BLUE | Receiving unframed all ones from the port; alarm indicator signal (AIS). |

### INTERFACES (DSX[3]) > STATUS > ALARMS > CLEAR HISTORY

Selecting this activator will clear the Alarm History for the T1 interface.

### INTERFACES (DSX[3]) > TEST

These options are used to initiate local and remote loopback tests and display the test status.

### INTERFACES (DSX[3]) > TEST > LOC LB

Loopback of the local unit. Choices are **NONE**, **LINE**, **AND PAYLOAD**. **LINE** Loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **PAYLOAD** Loopback  is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

### INTERFACES (DSX[3]) > TEST > REM LB

Loopback of remote unit. Choices are **NONE**, **LINE**, and **PAYLOAD**.  **LINE** Loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **PAYLOAD** Loopback is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

### INTERFACES (DSX[3]) > TEST > TEST STATUS

Indicates whether a test is in progress.

## INTERFACES (ETH[1])

View the Ethernet interface status and configure the Ethernet parameters from this menu.

NOTE *The 1 in ETH[1] represents a physical port. The Ethernet physical port is always 1.*

### INTERFACES (ETH[1]) > STATUS > MAC ADDRESS

This is a read-only field which displays the unique MAC address programmed at ADTRAN.

### INTERFACES (ETH[1]) > TEST > LOOPBACK

This option is used to initiate local a loopback on the Ethernet interface. The choices are **OFF** and **ON**. The default is **OFF**.

## INTERFACES (V35[2])

View the V.35 interface status and configure the V.35 parameters from this menu.

> NOTE *The 2 in V35[2] represents a physical port. The V.35 physical port is always 2.*

### INTERFACES (V35[2]) > CONFIG

Configure the DTE leads from this menu.

### INTERFACES (V35[2]) > CONFIG > CTS

Sets the control characteristic of the clear-to-send lead. Choices are **NORMAL** (follows RTS) or **FORCE ON.** Default is **NORMAL.**

### INTERFACES (V35[2]) > CONFIG > DCD

Sets the control characteristic of the carrier detect lead. Choices are **NORMAL** (follows valid signal on the network interface) or **FORCE ON.** Default is **NORMAL.**

### INTERFACES (V35[2]) > CONFIG > DSR

Sets the control characteristic of the data set ready lead. Choices are **NORMAL** (follows DTR) or **FORCE ON**. Default is **NORMAL.**

### INTERFACES (V35[2]) > STATUS

View the status of the DTE leads from this menu.

### INTERFACES (V35[2]) > STATUS > RTS

View the status of Request to Send (RTS) lead. Possibilities are **OFF** or **ON**. This is a read-only field.

### INTERFACES (V35[2]) > STATUS > DTR

View the status of the Data Terminal Read (DTR) lead. Possibilities are **OFF** and **ON**. This is a read only field.

### INTERFACES (V35[2]) > STATUS > TEST

Initiate a local loopback testing from this menu.

### INTERFACES (V35[2]) > TEST > LOOPBACK

This initiates a local loopback towards the DTE when set to **ON**. The default is **OFF**.

## INTERFACES (FXS)

View the FXS interface status and configure the FXS parameters from this menu.

### INTERFACES (FXS) > CONFIG

Configure the FXS mode, line impedance and Tandem parameters from this menu.

### INTERFACES (FXS) > CONFIG > SLOT

Indicates the slot to which the FXS is installed.

### INTERFACES (FXS) > CONFIG > PORT

Indicates the port on which the FXS is installed.

### INTERFACES (FXS) > CONFIG > MODE

Choices are given below. Default is **LOOP START.**

> *This mode needs to be set based on how the network is set up and how each port is being used. Each port does not need to be set to the same mode.*

**LOOP START** Sets the port to use FXS loop start signaling on the T-span and loop start supervision on the analog 2-wire interface.

**GROUND START** Sets the port to use FXS ground start signaling on the T-span and ground start supervision on the analog 2-wire interface.

### INTERFACES (FXS) > CONFIG > TX (dB)

Sets the TX direction level points. This signal will change the volume of the voice. TX (dB) is the signal that is transmitted out the T1, with 0 dB being the strongest. If the volume is too loud across the T1, this number should be increased. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **6.0 dB**.

### INTERFACES (FXS) > CONFIG > RX (dB)

Sets the RX direction level points. This signal will change the volume of the voice. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **3.0 dB**. The maximum signal is 0.0. dB.

### INTERFACES (FXS) > CONFIG > SVC MODE

Indicates whether the module is **IN SERVICE** or **OUT OF SVC**. This does not indicate whether the port has been mapped. For proper operation, the port must be mapped using the **DS0 MAPS** menu. Default is **IN SERVICE.**

### INTERFACES (FXS) > CONFIG > CODING TYPE

This is a read-only field which displays module code type.

### INTERFACES (FXS) > CONFIG > LINE Z

Sets the line impedance. Choices are **600 OHMS, 900 OHMS, 600 OHMS + 2.16µF, 900 OHMS + 2.16µF,** and **AUTO**. The line impedance of each port is based on the size of the network. Default is **600 OHMS**.

### INTERFACES (FXS) > CONFIG > MSG IND

This is better referred to as On-Hook Message Waiting. When this is set to **ENABLE,** talk path is always open, even in On-Hook conditions, in order for these FXS message tones to pass through. Default is **DISABLE**. Enabling on-hook message waiting will allow message lamp usage but will cause a lower on-hook voltage. Disabling this feature will allow higher on-hook voltage but will not allow on-hook messaging other than caller ID.

### INTERFACES (FXS) > STATUS

Displays the status of the FXS signal bits.

### INTERFACES (FXS) > STATUS > SLOT

Indicates the slot in which the FXS is installed.

### INTERFACES (FXS) > STATUS > PORT

Displays the port number.

### INTERFACES (FXS) > STATUS > TA SIG

This parameter displays the status of the Transmit A signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXS) > STATUS > TB SIG

This parameter displays the status of the Transmit B signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXS) > STATUS > RA SIG

This parameter displays the status of the Receive A signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXS) > STATUS > RB SIG

This parameter displays the status of the Receive B signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXS) > TEST

Activate tests and monitor test status on a per port basis from this menu.

### INTERFACES (FXS) > TEST > SLOT

Indicates the slot in which the FXS is installed.

### INTERFACES (FXS) > TEST > PORT

Displays the port number.

### INTERFACES (FXS) > TEST > TEST

Choices are given below. Default is **NONE**.

**NONE** Indicates that no test is currently active.

**DIGITAL NETWORK LPBK** Used to loop back DS0 data coming from the network for each channel. Received data is latched in on the appropriate receive time slot on the receive bus. This data is then placed on the transmit bus in the unit's transmit time slot.

**NETWORK ON HOOK TEST** Used to test signaling sent to the network by the unit. On-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

**NETWORK OFF HOOK TEST** Used to test signaling sent to the network by the unit. Off-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

**1 KHZ TONE-NEAR END** For Near End, the 2-wire side sends out a 1 kHz tone to verify talk path.

**1 KHZ TONE-FAR END** For Far End, the tone side is sent out across the Network and can be heard if monitoring on the T1 as well as off of the Far End 2-wire side. This verifies talk path.

**CUSTOMER RING TEST** The customer ring test will activate the unit's ring relay in a 2-on /4-off cadence, providing ringing to the customer loop.

### INTERFACES (FXS) > TEST > TEST STATUS

This option indicates whether a test is in progress.

## INTERFACES (FXO)

View the FXS interface status and configure the FXS parameters from this menu.

### INTERFACES (FXO) > CONFIG

Configure the FXS mode, line impedance, and Tandem parameters from this menu.

### INTERFACES (FXO) > CONFIG > SLOT

Indicates the slot in which the FXS is installed.

### INTERFACES (FXO) > CONFIG > PORT

Indicates the port on which the FXS is installed.

### INTERFACES (FXO) > CONFIG > MODE

Choices are given below. Default is **LOOP START.**

> NOTE *This mode needs to be set based on how the network is set up and how each port is being used. Each port does not need to be set to the same mode.*

**LOOP START** Sets the port to use FXO loop start signaling on the T-span and loop start supervision on the analog 2-wire interface.

**GROUND START** Sets the port to use FXO ground start signaling on the T-span and ground start supervision on the analog 2-wire interface.

**DPO** Sets the port to use Dial Pulse signaling to originate dialed numbers.

### INTERFACES (FXO) > CONFIG > TX (dB)

Sets the TX direction level points. This signal will change the volume of the voice. TX (dB) is the signal that is transmitted out the T1, with 0 dB being the strongest. If the volume is too loud across the T1, this number should be increased. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **0.0 dB**.

### INTERFACES (FXO) > CONFIG > RX (dB)

Sets the RX direction level points. This signal will change the volume of the voice. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **0.0 dB**.

### INTERFACES (FXO) > CONFIG > SVC MODE

Indicates whether the module is **IN SERVICE** or **OUT OF SVC**. This does not indicate whether the port has been mapped. For proper operation, the port must be mapped using the **DS0 MAPS** menu. Default is **IN SERVICE.**

### INTERFACES (FXO) > STATUS

Displays the status of the FXO signal bits.

### INTERFACES (FXO) > STATUS > PORT

Displays the port number.

### INTERFACES (FXO) > STATUS > TA SIG

This parameter displays the status of the Transmit A signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXO) > STATUS > TB SIG

This parameter displays the status of the Transmit B signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXO) > STATUS > RA SIG

This parameter displays the status of the Receive A signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXO) > STATUS > RB SIG

This parameter displays the status of the Receive B signal bit. The high/low status is indicated by a 0 or 1.

### INTERFACES (FXO) > TEST

Activate tests and monitor test status on a per port basis from this menu.

### INTERFACES (FXO) > TEST > SLOT

Indicates the slot in which the FXS is installed.

### INTERFACES (FXO) > TEST > PORT

Displays the port number.

### INTERFACES (FXO) > TEST > TEST

Choices are given below. Default is **NONE**.

**NONE** Indicates that no test is currently active.

**DIGITAL NETWORK LPBK** Used to loop back DS0 data coming from the network for each channel. Received data is latched in on the appropriate receive time slot on the receive bus. This data is then placed on the transmit bus in the unit's transmit time slot.

**NETWORK ON HOOK TEST** Used to test signaling sent to the network by the unit. On-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

**NETWORK OFF HOOK TEST** Used to test signaling sent to the network by the unit. Off-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.

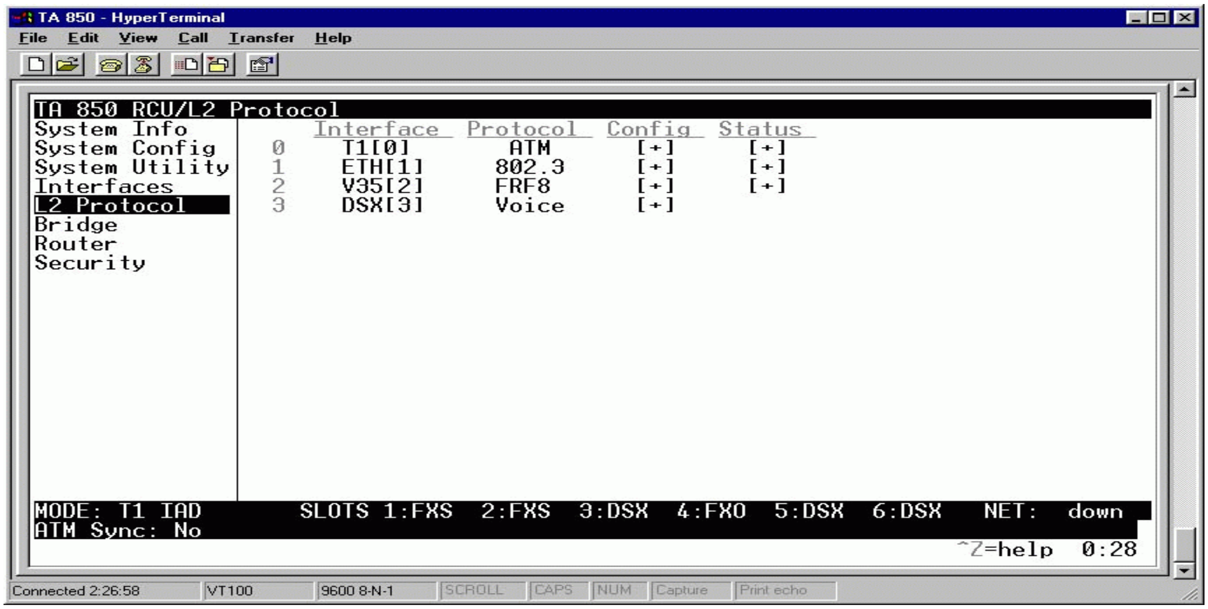
**1004 HZ - 0DCBM0 TONE GEN** Used to verify talk path by sending out 1004 Hz tone to test across the network. Monitoring of the T1 as well as the Far-End 2-wire side verifies the talk path if the tone is heard.

### INTERFACES (FXO) > TEST > TEST STATUS

This option indicates whether a test is in progress.

## L2 PROTOCOL

Use the L2 protocol menu to select the L2 protocol, configure the protocol specific parameters and view the status as shown in Figure 6.



```
TA 850 RCU/L2 Protocol
System Info        Interface   Protocol   Config   Status
System Config   0    T1[0]        ATM       [+]      [+]
System Utility  1    ETH[1]      802.3      [+]      [+]
Interfaces      2    V35[2]      FRF8       [+]      [+]
L2 Protocol     3    DSX[3]      Voice      [+]
Bridge
Router
Security

MODE: T1 IAD        SLOTS 1:FXS  2:FXS  3:DSX  4:FXO  5:DSX  6:DSX   NET:  down
ATM Sync: No
                                                               ^Z=help  0:28
```

**Figure 6. L2 Protocol Menu**

## L2 PROTOCOL (T1[0])

Configure the L2 Protocol parameters and view the status of the T1 interface using ATM protocol from this menu.

> *The 0 in T1[0] represents a physical port. The T1 physical port is always 0.*

### L2 PROTOCOL (T1[0]) > PROTOCOL

Configure the L2 protocol mode. Choices are **ATM** or **CUMTN FRE**. The default is ATM.

## L2 PROTOCOL (T1[0])>PROTOCOL> ATM

Asynchronous Transfer Mode allocates bandwidth on demand, automatically adjusting the network capacity to meet the system needs. Fixed-length cells (53 octet) require lower processing overhead and allow higher transmission speeds than traditional packet switching methods. ATM uses five octet headers in each fifty-three octet cell to match cells with specific virtual channels to which they belong.

> *Please see page 201 for the CopperMoutain protocol menu guide.*

### L2 PROTOCOL (T1[0] - ATM) > CONFIG

Configure the L2 Protocol parameters for the T1 interface using ATM protocol.

### L2 PROTOCOL (T1[0] - ATM) > CONFIG > ATM CONFIG

Use the ATM config menu to set the parameters listed below.

### L2 PROTOCOL (T1[0] - ATM) > CONFIG > ATM CONFIG > IDLE CELLS

The **IDLE CELLS** format must be configured for either **ATM FORUM (UNASSIGNED)** or **ITU (IDLE)**. Configuring this setting incorrectly for a particular circuit will cause poor performance at the ATM Layer. The default is **ATM FORUM (UNASSIGNED)**.

### L2 PROTOCOL (T1[0] - ATM) > CONFIG > ATM CONFIG > DATA SCRAMBLING

**DATA SCRAMBLING** can be **ENABLED** or **DISABLED** for cell traffic. Configuring this setting incorrectly for a particular circuit will cause poor performance at the ATM Layer.

> *The setting must match the configuration setting of the ATM switch or DSLAM at the other end of the circuit.*

### L2 PROTOCOL (T1[0] - ATM) > CONFIG > ATM CONFIG > HEC COSET

Header Error Control is located in the last (5th) byte of the ATM cell header that checks for cell integrity only. The Coset polynomial is applied to the received HEC for comparison with the HEC generated internally. HEC errors may be detected after synchronization any bit errors detected will prompt that cell be dropped. The choice are **ENABLED** or DISABLED. The default is **ENABLED**.

### L2 PROTOCOL (T1[0] - ATM) > CONFIG > PVC CONFIG

Configure up to six ATM PVCs from this menu (five data and one voice PVC).

### L2 PROTOCOL (T1[0] - ATM) > CONFIG > PVC CONFIG > NUM

Displays the index number for the PVC entry.

### L2 PROTOCOL (T1[0] - ATM) > CONFIG > PVC CONFIG > ACTIVE

Activates the ATM PVC. The choices are **YES** or **NO**. Default is **NO**.

### L2 PROTOCOL (T1[0] - ATM) > CONFIG > PVC CONFIG > SUB-INTERFACE

The T1 Sub-Interface is **ATM [0.0]** that represents the T1 physical and logical ports respectively. This is a read-only field.

### L2 PROTOCOL (T1[0] - ATM) > CONFIG > PVC CONFIG > VPI

ATM Virtual Path Identifier located in the ATM cell header identifies the virtual path over which this port is running. The range is **0-256**. The default is **0**.

### L2 PROTOCOL (T1[0] - ATM) > CONFIG > PVC CONFIG > VCI

This is the ATM Virtual Channel Identifier that serves as an address for the virtual channel cell transmissions between two devices. The range is **0-6535**. The default setting is **38**.

### L2 PROTOCOL (T1[0]-ATM) > CONFIG> PVC CONFIG > CONNECTION

Select the physical and logical method of data transfer over the virtual path.

*There are specific **SETUP** sub-menus for each **CONNECTION** choice. Each sub-menu is explained within the **ROUTER**, **V.35**, and **VOICE** configuration guides below.*

### L2 PROTOCOL (T1[0]-ATM) > CONFIG > PVC CONFIG > CONNECTION [ROUTER] > SETUP > PROTOCOL

Select the data-link protocol for the PVC. The choices are **IP** or **PPP**. The default is **IP**.

*The following **PPP SETUP** menu options only appear when the Protocol is set to **PPP**.*
*L2 Protocol [0] > Config > DVC Config > Setup > PPP Setup*

### AUTHENTICATION [+]

The **AUTHENTICATION** menu contains the required parameters for the authentication of the PPP peer and for being authenticated by the PPP peer. Authentication is applied between the unit and the PPP peer as described in the **AUTHENTICATION** submenus.

### TX METHOD

This parameter specifies how the unit is to be authenticated by the PPP peer. There are four possible selections. Default it **NONE**.

**NONE** The connection will not allow the PPP peer to authenticate it.

**PAP, CHAP, OR EAP** The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** or **PAP**.

**CHAP OR EAP** The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** but not **PAP**.

**EAP ONLY** The unit will only allow **EAP** to be negotiated. If the PPP peer is not capable of doing **EAP**, then the connection will not succeed.

**PAP ONLY** The unit will only allow **PAP** to be negotiated. If the PPP peer is not capable of doing **PAP**, then the connection will not succeed.

### RX METHOD

This parameter specified how the unit is to be authenticated by the PPP peer. There are four possible selections. Default is **NONE**.

**NONE** The connection will not allow the PPP peer to authenticate it.

**PAP, CHAP, OR EAP** The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** or **PAP**.

**CHAP OR EAP** The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** but not **PAP**.

**EAP** The unit will only allow **EAP** to be negotiated. If the PPP peer is not capable of doing **EAP**, then the connection will not succeed.

### PPP [0]

Configure the PPP specific parameters such as **MAX CONFIG**, **MAX TIMER**, **MAX FAILURE**, and **FORCE PEER IP ADDRESS** from this menu.

#### MAX CONFIG

This value is the number of unanswered configuration-requests that should be transmitted before resetting PPP negotiations. the possible values are **5**, **10**, **15**, and **20** (default).

#### MAX TIMER (SEC)

This value is the number of seconds to wait between unanswered configuration-requests. The possible values are **1 SEC**, **2 SECS**, **3 SECS (DEFAULT)**, **5 SECS**, and **10 SECS**.

#### MAX FAILURE

Due to the nature of PPP, configuration option may not be agreed upon between two PPP peers. This value is the number of configuration-naks that should occur before an option is configuration-rejected. The possible values are **5 (DEFAULT)**, **10**, **15**, and **20**.

#### FORCE PEER IP ADDRESS

This option forces the PPP to negotiate the IP address entered instead of allowing another address to be assigned by the remote end. The default is **NO**.

#### KEEPALIVE PERIOD

This option allows the user to generate PPP keepalive packets that can be sent every **1** minute, **2** minutes, or every **5** minutes. A value of **0 (OFF)** disables the PPP keepalive packet generating feature. The default is **0 (OFF)**.

#### PPP ENCAPSULATION

This option allows the user to set the encapsulation modes for PPP over ATM. LLC has an encapsulation header in the AAL5 frame indicating it is encapsulating PPP. VC-Mux does not have a header, and is therefor dedicated to using PPP. The choices are **LLC** or **VC-MUX**. The default is **VC-MUX**.

## L2 PROTOCOL (T1[0]-ATM) > CONFIG > PVC CONFIG > CONNECTION [ROUTER] > SETUP > MODE

This mode identifies how the data will be transferred. The choices are:

| | |
|---|---|
| **ROUTE IP** | All IP data for this PVC will be routed. |
| **BRIDGE ALL** | All data for this PVC will bridged. |
| **ROUTE IP/BRIDGE OTHER** | All IP data will be routed. All other data will be bridged. |

The default is **ROUTE IP**.

## L2 PROTOCOL (T1[0]-ATM) > CONFIG > PVC CONFIG > CONNECTION [V35] > SETUP

Use these menus to setup the Protocol Mapping, DE Map, and the FECN Map for the Router PVC connections.

### PROTOCOL MAPPING

Network providers have the ability to provision each PVC pair with an encapsulation mode to ensure interoperability between terminal equipment. The two modes are **TRANSPARENT** and **TRANSLATION** Translation mode is most common and carries multiple upper layer protocols over Frame Relay and ATM PVCs. The choices are **TRANSPARENT** or **TRANSLATION**. The factory default setting is **TRANSLATION.**

### DE MAP

Maps Frame Relay Discard Eligible (DE) bit to the ATM Cell Loss Priority (CLP) bit. The choices are **DE = 0**, **DE = 1**, and **CONVERT** (map DE TO CLP). The factory default setting is **DE = 0**.

### FECN MAP

Allows mapping of Frame Relay FECN (Forward Explicit Congestion Notification) bit to ATM EFCI (Explicit Forward Congestion Indicator) bit. The choices are **NO MAP FECN** and **MAP** FECN. The factory default setting is **NO MAP FECN**.

## L2 PROTOCOL (T1[0]-ATM) > CONFIG > PVC CONFIG > CONNECTION [V35] > SETUP > DLCI MAPPING

Use this menu to configure the DLCI mapping.

### MAP

Displays the DLCI Map number. This is a read-only field.

### ACTIVE

Enables FR/ATM mapping. The choices are **YES** or **NO**. The default is **YES**.

### INTERFACE

The T1 interface is **ATM[0.0]** which represents the T1 physical and logical ports respectively. This is a read-only field.

## L2 PROTOCOL (T1[0]-ATM) > CONFIG > PVC CONFIG > CONNECTION [VOICE] > SETUP

Use these menus to setup the **CALL CONTROL**, **LES PROFILE**, and the **LES-CAS** specific for the Voice PVC connections.

### CALL CONTROL

The Call Control setting is used to configure the correct Voice Gateway protocol for voice signaling control between the Total Access 850 and the configured Gateway. The **CALL CONTROL** setting must be configured correctly before the voice circuits will work correctly. The Total Access 850 supports Jetstream, Coppercom, Tollbridge, and LES-CAS. The default is LES-CAS.

### LES PROFILE

This options applies when **CALL CONTROL** is set to **LES-CAS**. The choices are **ITU PROFILE 1**, **ATM FORUM PROFILE 9**, and **ATM FORUM PROFILE 10**. The default is **ATM FORUM PROFILE 10**.

NOTE

***ATM FORUM PROFILE 9*** *provides ability to support 64 Kbps PCU calls.* ***ATM FORUM PROFILE 10*** *enables support of 64 Kbps PCU calls as well as 32 Kbps ADPCU calls.*

### LES-CAS GW SIM

Only use **ENABLED** when back-to-back IAD testing to simulate alive gateway. The choices are **ENABLED** or **DISABLED**. The default is **DISABLED**.

## L2 PROTOCOL (T1[0]-ATM) > CONFIG > PVC CONFIG > QOS

Quality of Service (**QOS**) for ATM UBR and VBR non-real time for the data PVC DLCI. The choices are **UBR** and **NRTVBR**. The factory default setting is **UBR**.

### L2 PROTOCOL (T1[0]-ATM) > CONFIG > PVC CONFIG > PCR

**PEAK CELL RATE** for ATM for the data PVC. **PCR** is normally used for UBR connections and can be calculated using the following equations. **PEAK CELL RATE** = Bit Rate/424 (The total of all PCRs must not exceed the line rate). The range is **0** to **3623**. The factory default setting is **3623**.

> *The* ***QOS*** *sub-menu above reflects* ***ROUTER*** *and* ***V.35 CONNECTION*** *settings only. The* ***VOICE CONNECTION QOS*** *option is a read-only field described below.*

### L2 PROTOCOL (T1[0]-ATM) > STATUS > ATM STATUS

#### AP: TX CELLS

This is the number of cells transmitted.

#### AP: RX CELLS

This is the number of cells received.

#### AP: RX OAM CELLS

This is the number of OAM cells received

#### AP: RECEIVE CELLS DISCARDED

This is the number of cells received and discarded. An incrementing count in this field could indicate a configuration problem with the ATM layer.

#### AP: RECEIVE CELL ERRORS

This is the number of cells received with an HEC error.

#### AP: SYNC

This indicates cell delineation at the ATM layer.

#### AP: OUT OF CELL DELINEATION

This indicates loss of cell delineation at the ATM layer.

#### AAL5: TRANSMIT FRAMES

This is the number of AAL5 frames transmitted.

#### AAL5: RECEIVE FRAMES

This is the number of AAL5 frames received.

### AAL5: Transmit Discarded Frames

This is the number of AAL5 frames discarded.

### AAL5: Receive Errors

This is the number of AAL5 errors received.

### AAL5: Receive Discarded Frames

This is the number of AAL5 frames received from the network that have been discarded.

### AAL5: No ATM Frames

This is for internal use only.

### AAL5: No Data Packets

This is for internal use only.

### Clear Stats

This is used to clear the counters on this menu screen.

### L2 Protocol (T1[0]-ATM) > Status > PVC Status

View the ATM PVC statistics from this menu.

### L2 Protocol (T1[0]-ATM) > Status > PVC Status > Num

Displays the index number in the PVC Status menu.

### L2 Protocol (T1[0]-ATM) > Status > PVC Status > Sub-Interface

The T1 **Sub-Interface** is **ATM[0.0]** that represents the T1 physical and logical ports respectively. This is a read-only field.

## L2 PROTOCOL (T1[0]-ATM) > STATUS > PVC STATUS > AAL STATS

Shows the statistics of ATM Adaptation Layer frames.

| | |
|---|---|
| **MAX PDU SIZE** | Maximum Protocol Data Unit size for the ATM AAL5 frame. |
| **TX DATA BYTES** | Number of AAL5 data bytes transmitted. |
| **TX FRAMES** | Number of AAL5 frames transmitted. |
| **TX CELLS (ALL TYPES)** | Total number of AAL5 cells transmitted (all types). |
| **TX OAM CELLS** | Number of AAL5 Operations, Administration, and cells transmitted. |
| **TX RM CELLS** | Number of AAL5 RM cells transmitted. |
| **TX EFCI=1 CELLS** | Number of AAL5 EFCI=1 cells transmitted. |
| **TX CLPI=1 CELLS** | Number of AAL5 CLPI=1 transmitted. |
| **RX DATA BYTES** | Number of AAL5 data bytes received. |
| **RX FRAMES** | Number of AAL5 frames received |
| **RX USER CELLS** | Number of AAL5 user cells received |
| **RX OAM CELLS** | Number of AAL5 OAM cells received |
| **RX BAD OAM CELLS** | Number of AAL5 Bad OAM cells received |
| **RX RM CELLS** | Number of AAL5 RM cells received |
| **RX BAD RM CELLS** | Number of AAL5 Bad RM cells received |
| **RX EFCI=1 CELLS** | Number of AAL5 EFCI=1 cells received. |
| **RX CLPI=1 CELLS** | Number of AAL5 CLPI=1 cells received. |
| **DISCARD RX CELLS** | Number of AAL5 RX cells which were discarded. |
| **DISCARD RX FRAMES** | Number of AAL5 RX frames which were discarded. |
| **DISCARD TX FRAMES** | Number of AAL5 TX frames which were discarded. |
| **TX QUEUE OVERFLOW** | Number of cells discarded due to queue overflow. |

**TX OUT OF CELLS** Number of AAL5 TX Out of Cells.

**TX INACTIVE** Number of TX frames discarded while PVC is inactive.

**RX INACTIVE** Number of RX frames discarded while PVC is inactive.

**CRC ERRORS** Number of AAL5 CRC Errors.

**REASSEMBLY TIMEOUTS** Number of AAL5 Reassembly Timeouts.

**TOO LONG FRAMES** Number of AAL5 Too Long Frames.

**CLEAR COUNTS** Select to clear counters.

## L2 PROTOCOL (T1[0]-ATM) > STATUS > PVC STATUS > PROTOCOL STATUS

Use these menus to view the **AAL2 STATS**, **POTS STATS**, and to **CLEAR STATS** for the PVC Protocol.

### AAL2 STATS

ATM Adaptation Layer 2 statistics is used to provide error information on voice traffic. This menu displays **RX AAL2 HEC ERRORS**, **RX AAL2 SEQK ERRORS**, **RX VOICE SEQ ERRORS**, **RX VOICE BAD CID**, **RX VOICE BAD UUI**, **RX VOICE EOC CELLS**, and **PEAK CELL RATE**.

### POTS STATS

Selecting this menu options will show real time indication status of each voice port on the Total Access 850. On a per port basis, the user can determine which ports are active/inactive as well as view other statistics like **TXQ**, **INSERTS** and **DROPS INDICATORS**.

NOTE

*The Echo Canceller module ADPCM functionality automatically shifts ON/OFF when fax or modem calls are placed. To find out the current status of the Echo Canceller functionality, check the current status of each FXS port. The path of the current status can be found at the following path:* ***L2 PROTOCOL > STATUS > PVC STATUS > PROTOCOL STATUS > POTS STATS > CODING TYPE*** *(this will display either PCM of ADPCM).*

### CLEAR STATS

The Clear Stats option is used to clear the statistic counters.

## L2 PROTOCOL (T1[0]) > PROTOCOL> CUMTN FRE

Copper Mountain Frame Relay is a data link layer protocol that uses Frame Relay instead of ATM on the subscriber loop. Frame relay is a switched layer protocol that handles virtual circuits using High-Level Data Link Control (HDLC) encapsulation. Frame Relay uses statistical multiplexing as opposed to time-division-multiplexing many logical connections over a single physical link.

*To insert a new profile, press the* **I** *key when over the* **NUM** *column. A new inserted profile will always be set up with the default parameters. To copy parameters from an old profile to this newly inserted profile, use the copy (***C***) and paste (***P***) keys. Entire configuration trees can be copied with this method.*

*To delete an unused profile, use the* **D** *key when the cursor is over the number in the* **NUM** *column. Once deleted, the profile is gone permanently.*

### L2 PROTOCOL (T1[0] - CUMTN) > CONFIG > NUM

Displays the index number in the DLCI config table. The number range is 0-9.

### L2 PROTOCOL (T1[0] - CUMTN) > CONFIG > ACTIVE

When this parameter is set to **YES** (def), the mapping is used to determine the protocols used. If set to **NO,** the unit will ignore the virtual circuit with this DLCI.

### L2 PROTOCOL (T1[0] - CUMTN) > CONFIG > INTERFACE

Shows the user the physical and logical port associated with each DLCI. This is a read-only field.

### L2 PROTOCOL (T1[0] - CUMTN) > CONFIG > DLCI

The DLCI (Data Link Connection Identifier) number identifies the virtual circuit being configured. The DLCI range is 16-1023. The default is 16-25 corresponding to the index numbers 0-9 respectfully.

### L2 PROTOCOL (T1[0] - CUMTN) > CONFIG > CONNECTION

The mode identifies how the data will be forwarded and shows the user the physical type of connection associated with the DLCI. The profile displays **ROUTER** or **VOICE** connection.

### L2 PROTOCOL (T1[0] - CUMTN) > CONFIG > SETUP

This submenu only appears for Voice connections. Configure the **CALL CONTROL** for voice gateway.

## L2 PROTOCOL (T1[0] - CUMTN) > CONFIG > SETUP > CALL CONTROL

The **CALL CONTROL** setting is used to configure the correct Voice Gateway protocol for voice signaling control between the Total Access 850 and the configured Gateway. The Call Control setting must be configured correctly before the voice circuits will work correctly. The Total Access 850 supports **JETSTREAM**, **COPPERCOM**, **TOLLBRIDGE** and **LES-CAS**. The default is **LES-CAS**.

## L2 PROTOCOL (T1[0] - CUMTN) > STATUS

View the status of the Copper Mountain DLCI connections.

## L2 PROTOCOL (T1[0] - CUMTN) > NUM

Displays the index number for the Status menu entries.

## L2 PROTOCOL (T1[0] - CUMTN) > STATUS > SUB-INTERFACE

The T1 **SUB-INTERFACE** is CuMtn[0.0] when the L2 Protocol is set for **CUMTN FRE**. The [0.0] represents the T1 physical and logical ports respectively. This is a read-only field.

## L2 PROTOCOL (TQ[0]-CUMTN) > STATUS> DLCI STAT

This is a read-only field that displays the live DLCI state.

## L2 PROTOCOL (T1[0]-CUMTN) > STATUS > PROTOCOL STATUS

This is a read-only field that displays the live protocol status. Menu visible for physical and logical **VOICE** ports only.

### POTS STATS

View the voice port activity and coding type.

### CLEAR STATS

Selecting the option will clear the voice port statistics.

## L2 PROTOCOL (ETH[1])

Configure the **L2 PROTOCOL** parameters and view the status of the Ethernet interface from this menu.

### L2 PROTOCOL (ETH[1]) > INTERFACE

The 1 in ETH[1] represents a physical port. The Ethernet physical port is always 1.

### L2 PROTOCOL (ETH[1]) > PROTOCOL

Displays the L2 protocol for the 10/100BaseT Ethernet port. Currently only **802.3** is supported.

### L2 PROTOCOL (ETH[1]) > CONFIG

Configure the mode for this **10/100BASET** Ethernet port from this menu.

### L2 PROTOCOL (ETH[1]) > CONFIG > MODE

The mode identifies how the data will be forwarded. The choices are:

| | |
|---|---|
| **ROUTE IP** | All IP data will be routed |
| **BRIDGE ALL** | All data will be bridged |
| **ROUTE IP/BRIDGE OTHER** | All IP data will be routed. All other data will be bridged. |

The default is **ROUTE IP.**

### L2 PROTOCOL (ETH[1]) > STATUS

View the L2 protocol statistics for the **10/100BASET** Ethernet port from this menu.

### L2 PROTOCOL (ETH[1]) > STATUS > TX PACKETS

Total number of packets transmitted out the Ethernet port.

### L2 PROTOCOL (ETH[1]) > STATUS > RX PACKETS

Total number of packets received from the Ethernet port.

### L2 PROTOCOL (ETH[1]) > STATUS > TX ERRORS

Total number of transmit errors encountered on Ethernet port.

### L2 PROTOCOL (ETH[1]) > STATUS > SINGLE COLLISIONS

Total number of single collisions before successful transmission.

### L2 PROTOCOL (ETH[1]) > STATUS > MULTIPLE COLLISIONS

Total number of multiple collisions before successful transmission.

### L2 PROTOCOL (ETH[1]) > STATUS > EXCESSIVE COLLISIONS

Total number of collisions that resulted in packet being dropped.

### L2 PROTOCOL (ETH[1]) > STATUS > DEFERRED TRANSMISSIONS

Total number of packets deferred due to collisions.

### L2 PROTOCOL (ETH[1]) > STATUS > CARRIER SENSE ERRORS

Total number of carrier sense errors encountered (no link integrity).

### L2 PROTOCOL (ETH[1]) > STATUS > RX ERRORS

Number of packets received in error and dropped.

### L2 PROTOCOL (ETH[1]) > STATUS > CRCS

Number of packets detected with CRC errors.

### L2 PROTOCOL (ETH[1]) > STATUS > RX COLLISIONS

Number of collisions which occurred during reception.

### L2 PROTOCOL (ETH[1]) > STATUS > NON-ALIGNED

The **NON-ALIGNED** parameter is set when the number of bits received is not divisible by 8.

### L2 PROTOCOL (ETH[1]) > STATUS > CLEAR COUNTS

Selecting this activator clears all the Ethernet stats.

## L2 PROTOCOL (V35[2]-ATM)

View the V.35 interface configuration from this menu.

### L2 PROTOCOL (V35[2]-ATM) > INTERFACE

The 2 in V35[2] represents a physical port. The V.35 physical port is always 2.

### L2 PROTOCOL (V35[2]-ATM) > PROTOCOL

The Protocol setting configures the V.35 port for FRF5 or FRF8 operation, depending upon the application being supported.

**FRF5**

This is also known as Network Interworking. Use this mode for Frame Relay over ATM.

**FRF8**

This is also known as Service Interworking. In this mode, the unit performs a translation between Frame Relay and ATM protocols.

The factory default setting is FRF5.

### L2 PROTOCOL (V35[2]-ATM)> CONFIG

These configuration options are available when the Protocol is set to FRF 5 or FRF8.

### L2 PROTOCOL (V35[2]-ATM) > CONFIG > UNI MAINT PROTOCOL

Specifies the maintenance protocol or signaling protocol between the local V.35 port and the attached DTE port. The choices are ANNEX D, ANNEX A, LMI, and STATIC. The factory default setting is ANNEX D.

### L2 PROTOCOL (V35[2]-ATM) > CONFIG > UNI POLL TIMEOUT T392 (5-30)

T392 for signaling protocol. This parameter has no meaning if the UNI Maint Protocol is set to STATI C (no signaling). The default setting is 10.

### L2 PROTOCOL (V35[2]-ATM)> STATUS

These stats are available when the Protocol is set to FRF5 or FRF8.

## L2 Protocol (V35[2]-ATM)> Status> Port

**Port Index** Port number.

**Signal State** Frame relay state.

**Tx Frames** Number of frames transmitted.

**Rx Frames** Number of frames received.

**Tx Bytes** Number of bytes transmitted.

**Rx Bytes** Number of bytes received.

**Full Status TX Frames** Number of Frame Relay signaling packets transmitted out the port.

**Full Status RX Frames** Number of Frame Relay signaling packets received by the port.

**Link Integrity Status TX Frames** Number of Link Integrity signaling packets transmitted outport.

**Link Integrity Status RX Frames** Number of Link Integrity signaling received by the outport.

**Drop Unknown DLCI** Number of frames received that were not associated with any known PVC.

**Drop Invalid DLCI** Number of frames received that had illegal DLCIs.

**Clear Stats** When activated, this field will clear all frame relay port stats.

## L2 Protocol (V35[2]-ATM)> Status> PVC(s)

**DLCI** DLCI number.

**State** Frame relay state.

**Tx Frames** Number of frames transmitted.

**Rx Frames** Number of frames received.

**Rx Bytes** Number of bytes received.

**DE Count** Number of packets received on an individual DLCI with the DE bit set.

**CR Count** Number of packets received on an individual DLCI with the CR bit set.

**BECN Count** Number of packets received on an individual DLCI with the BECN bit set.

**FECN Count** Number of packets received on an individual DLCI with the FECN bit set.

**Unknown Frame** RX Frames received that were not associated with any PVC entries.

## INTERFACES (DSX[3])

Configure T1 parameters from this menu.

### INTERFACES (DSX[3] - VOICE) > INTERFACE

The 3 in DSX[3] represents a physical port. The DSX1 physical port is always 3.

### INTERFACES (DSX[3]) > CONFIG

Configure the various DSX1 signaling from this menu.

### INTERFACES (DSX[3]) > CONFIG > SIGNALING

The signaling needs to be configured based on the network application. The choices are:

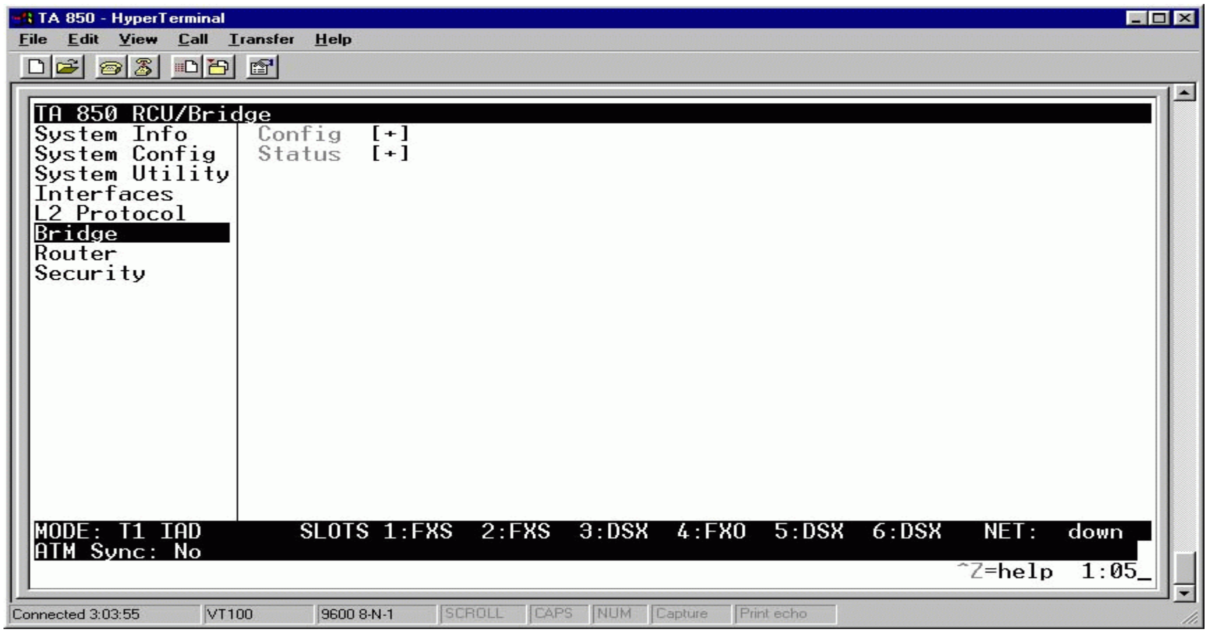
| | |
|---|---|
| **E&M (TANDEM)** | Sets the DSX interface to use E&M signaling. |
| **LOOP START** | Sets the DSX interface to use loop start signaling. |
| **GROUND START** | Sets the DSX interface to use ground start signaling. |
| **ISDN PRI** | Sets the DSX interface to use common channel signaling for ISDN. |

### INTERFACES (DSX[3]) > CONFIG > LEGACY CONFIG

Use **DSX CID** from 65. Digital trunk bearer channel CIDs that start from 65, otherwise select **IDLE REFRESH ALL**. The default is **DSX CID FROM 65, IDLE REFRESH ALL**.

## BRIDGE

Configure the bridge parameters and view bridging statistics from this menu as shown in Figure 7.



```
TA 850 RCU/Bridge
System Info       Config   [+]
System Config     Status   [+]
System Utility
Interfaces
L2 Protocol
Bridge
Router
Security

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:DSX  4:FXO  5:DSX  6:DSX   NET:  down
ATM Sync: No
                                                               ^Z=help  1:05_
```

**Figure 7. Bridge Menu**

### BRIDGE > CONFIG

Configure the interfaces and bridge table parameters from this menu.

### BRIDGE > CONFIG > INTERFACES (T1[0])

Configure the T1 interface bridging parameters from this menu.

### BRIDGE > CONFIG > BRIDGE TABLE

Configure the bridge table parameters from this menu.

### BRIDGE > CONFIG > BRIDGE TABLE > BRIDGE TABLE AGING (0-65535)

**BRIDGE TABLE AGING** is how soon an entry ages out of the Bridge table (in minutes). Default is 5.

### BRIDGE > STATUS

View the bridging statistics from this menu.

### BRIDGE > STATUS > BRIDGE TABLE

View the bridge table status from this menu.

### Bridge > Status > Bridge Table > MAC Address

Ethernet address for device learned. This is a read-only field.

### Bridge > Status > Bridge Table > Location

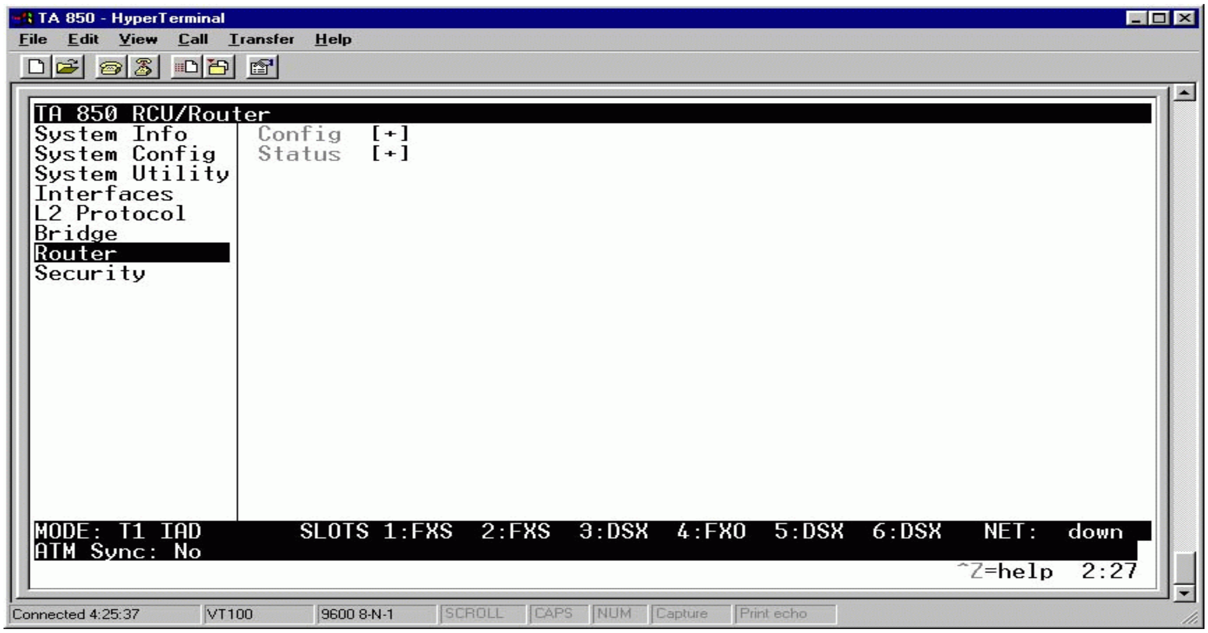
Location indicates if it is LAN or WAN. This is a read-only field.

### Bridge > Status > Bridge Table > TTL

Time to Live (TTL) is the number of seconds until the address is removed from the table. This is a read only field.

## Router

Configure the router parameters and view routing statistics from this menu as shown in Figure 8.



```
TA 850 RCU/Router
System Info      Config    [+]
System Config    Status    [+]
System Utility
Interfaces
L2 Protocol
Bridge
Router
Security

MODE: T1 IAD        SLOTS 1:FXS  2:FXS  3:DSX  4:FXO  5:DSX  6:DSX   NET:  down
ATM Sync: No
                                                                ^Z=help  2:27
```

**Figure 8. Router Menu**

### Router > Config

Configure the interfaces, routes, DHCP Server, and UDP Relay options from this menu.

### Router > Config > Interfaces

Configure the layer 3 options for the Ethernet and T1 interfaces from this menu.

### Router > Config > Interfaces (ETH[1])

Configure the layer 3 options for the Ethernet parameters from this menu.

NOTE *The 1 in ETH[1] represents a physical port. The Ethernet physical port will always be 1.*

NOTE *The Ethernet port will always appear in the* ***ROUTER > CONFIG > INTERFACES*** *table regardless of the L2 protocol mode setting.*

## ROUTER > CONFIG > INTERFACES (ETH[1]) > SUB-INTERFACE

The Ethernet sub-interface is 802.3[1.0]. The [1.0] represents the Ethernet physical and logical ports, where 1 is the physical port and 0 is the logical port assigned to the Ethernet interface. This is a read-only field.

## ROUTER > CONFIG > INTERFACES (ETH[1])> SETUP

Configure the Ethernet addressing, RIP, and Proxy ARP from this menu.

### PRIMARY IP

This is used to setup the IP addresses for the LAN on the unit.

#### IP ADDRESS

The IP address assigned to the unit's Ethernet port is set here. This address must be unique within the network. Default is **10.0.0.1**.

#### SUBNET MASK

This is the IP network mask that is to be applied to the unit's Ethernet port. Default is **255.255.255.0.**

#### RIP

Use this menu to enable RIP on the LAN interface.

##### VERSION

Enables or disables RIP and specifies the RIP protocol. Choices are; **OFF** (which disables RIP), **V1** (RIP Version 1) or **V2** (RIP Version 2). The default is **OFF**.

##### METHOD

Specifies the way the RIP protocol sends out its advertisements. The following options are available:

**SPLIT HORIZON (DEF)** Only routes not learned from this circuit are advertised.

**POISON REVERSE** All routes are advertised, but the routes learned from this port are “poisoned” with an infinite metric. The default is Split Horizon.

#### DIRECTION

Allows the direction at which RIP advertisements are sent and received to be specified.

**TX AND RX (DEF)** RIP advertisements are periodically transmitted and are listened to on this port.

**TX ONLY** RIP advertisements are periodically transmitted but are not listened to on this port.

**RX ONLY** RIP advertisements are listened to on this port, but are not transmitted on this port.

#### V2 SECRET

Enter the secret used by RIP version 2 here.

### PROXY ARP

This feature allows the network portion of a group of addresses to be shared among several physical network segments. The ARP protocol provides a way for devices to create a mapping between physical addresses and logical IP addresses. Proxy ARP makes use of this mapping feature by instructing a router to answer ARP requests as a "proxy" for the IP addresses behind one of its ports. The device which sent the ARP request will then correctly assume that it can reach the requested IP address by sending packets to the physical address that was returned. This technique effectively hides the fact that a network has been (further) subnetted. If this option is set to **YES,** when an ARP request is received on the Ethernet port the address is looked up in the IP routing table. If the forwarding port is not on the Ethernet port and the route is not the default route, the unit will answer the request with its own hardware address. Default is **NO**.

## SECONDARY IPS

This allows the unit to specify additional IP addresses and networks on its Ethernet. The maximum number of entries is 5.

### NUM

Displays the index number in the secondary IP list.

#### IP ADDRESS

This is the second IP address the unit will respond to on the Ethernet. Default is **0.0.0.0**.

#### SUBNET MASK

This is the mask for the network. Default is **255.255.255.255**.

#### NAT MODE

This mode specifies whether Network Address Translation (NAT) should be use on this interface. When this mode is set to **PRIVATE** (def) NAT is automatically specified on this interface. The other choice is **PUBLIC** which specifies **not** going through NAT.

### ROUTER > CONFIG > INTERFACES (ETH[1]) > SUB-INTERFACE

The Ethernet sub-interface is ATM[0.1]. The [0.1] represents the ATM physical and logical ports, when 0 is the physical port and 1 is the logical port assigned to the ATM interface. This a read-only field.

### ROUTER > CONFIG > INTERFACES (T1[0]) > SETUP

Configure the ATM pvc addressing, RIP, and NAT from this menu.

#### ACTIVE

This Selection enables IP on this PVC.

#### VPI

ATM virtual port identifier.

#### VCI

This is the ATM virtual channel identifier.

#### ADDRESS MODE

**USER SPECIFIED** allows the user configuration for Local IP and Far-End IP addresses, **DHCP CLIENT** is used for the Total Access 850 to learn his IP address from a DHCP server. The choices are **USER SPECIFIED** or **DHCP CLIENT**. The Default is **USER SPECIFIED**.

#### LOCAL IP ADDRESS

This is the IP address for this PCV.

#### FAR-END IP ADDRESS

This is the address of the NEXT hop router on this interface.

### IP NETMASK

This is the network mask used for this interface.

### NAT

Use this menu to set up and use Network Address Translation on this interface.

**PORT TRANSLATION** By enabling port translation, IP packets are modified as they pass through this interface. During transmission, private addresses are translated into a single public (NAPT) IP address. Incoming packets are translated from the public to private address based on the protocol port numbers. Once enabled, you must set up NAT for use. The default is **DISABLED**.

**PUBLIC IP ADDRESS MODE** The port translation requires at least a single real IP address for translating. This value can use the IP assigned to the interface (or assigned via layer 2 protocol like PPP), obtained using DHCP client, or statistically specified on this menu. If the address cannot be learned, then it must be specified in order for the translation to work.

**TRANSLATE BODY OF UNMAPPED PARTS** By default, the application payload in the packet is scanned for occurrences of the private/public IP address in binary or ASCII form. Set this to **DISABLED** for applications where this will cause problems.

**TRANSLATION TABLE** Add translation entries to “fine tune” special protocols or specify private addresses.

**NAT VIEW** Shows the protocols that are actively being translated.

**NAPT ADDRESS** Represents the public address that is being used as the NAPT address.

**ENTRY COUNT** The number of entries in the NAT table.

**ENTRY OVERFLOW COUNT** A count of the dropped entries due to low memory.

### RIP

Use this menu to set up and use Network Address Translation on this interface.

#### VERSION

Enables or disables RIP and specifies the RIP protocol. Choices are: **OFF** (which disables RIP), **V1** (RIP Version 1) or **V2** (RIP Version 2). The default is **OFF**

#### METHOD

Specifies the way the RIP protocol sends out its advertisements. The following options are available:

| | |
|---|---|
| **SPLIT HORIZON (DEF)** | Only routes not learned from this circuit are advertised. |
| **POISON REVERSE** | All routes are advertised, but the routes learned from this port are “poisoned” with an infinite metric. The default is Split Horizon. |

#### DIRECTION

Allows the direction at which RIP advertisements are sent and received to be specified.

### ROUTER > CONFIG > ROUTES

Configures the default gateway and static routes from this menu.

### ROUTER > CONFIG > ROUTES > DEFAULT GATEWAY

The default gateway is used by the unit to send IP packets whose destination addresses are not found in the route table. Default is **0.0.0.0.** This is a default gateway for the entire unit, not just for the Ethernet port.

### ROUTER > CONFIG > ROUTES > STATIC ROUTES

Use this menu to enter static routes to other networks.

#### NUM

Displays the index number in the static route table.

#### ACTIVE

Adds this static route entry to the IP routing table when set to **YES** and removes it (if it was previously added) if set to **NO**. Default is **NO**.

#### IP ADDRESS

The IP address of the host or network address of the device being routed to. Default is **0.0.0.0**.

#### SUBNET MASK

Determines the bits in the previous IP address that are used. If this is to be a host route, it must be set to all ones (255.255.255.255). Default is **0.0.0.0**.

#### GATEWAY

The IP address of the router to receive the forwarded IP packet. Default is **0.0.0.0.**

#### HOPS

The number of router hops required to get to the network or host. Maximum distance is 16 hops. Default is **1**.

#### PRIVATE

When set to **NO**, the unit will advertise this static route using RIP. Setting to **YES** means that the route is kept private. Default is **NO**.

### ROUTER > CONFIG > DHCP SERVER

Use this menu to set up the DHCP server.

### ROUTER > CONFIG > DHCP SERVER > DHCP MODE

When set to **ON**, the unit acts as a DHCP server and will dynamically assign IP, network mask, default gateway, and DNS addresses to any device which transmits a broadcast DHCP request. The addresses assigned are based on the unit's own IP address and will be within the same network. Default is **OFF.**

### ROUTER > CONFIG > DHCP SERVER > DHCP RENEWAL TIME (HOURS)

The number of hours that the DHCP server should allow the device to keep its previous IP assignment, before it is required to send a new DHCP request. The default is **0 HOURS** which represents an infinite lease.

### ROUTER > CONFIG > DHCP SERVER > DOMAIN NAME

Text string used to represent the domain name used by the unit.

### ROUTER > CONFIG > DHCP SERVER > PRIMARY DNS

First server to which domain name requests are sent.
Default is 0.0.0.0.

### ROUTER > CONFIG > DHCP SERVER > SECONDARY DNS

Server used as a backup, in case the primary address does not respond to the request.
Default is 0.0.0.0.

### ROUTER > CONFIG > DHCP SERVER > PRIMARY NBNS/WINS

Primary address of the NBNS/WINS server.
Default is 0.0.0.0.

### ROUTER > CONFIG > DHCP SERVER > SECONDARY NBNS/WINS

Secondary address of the NBNS/WINS server.
Default is 0.0.0.0.

### ROUTER > CONFIG > UDP RELAY

This menu configures the unit to act as a UDP relay agent for applications requiring a response from UDP hosts that are not on the same network segment as their clients.

### ROUTER > CONFIG > UDP RELAY > MODE

When this option is set to **ON**, the unit will act as a relay agent. Default is **OFF**.

### ROUTER > CONFIG > UDP RELAY > UDP RELAY LIST

Up to four relay destination servers can be specified in this list.

#### #

Indicates the entry number in the UDP Relay List table.

#### RELAY ADDRESS

This is the IP address of the server that will receive the relay packet. Default is **0.0.0.0**.

#### UDP PORT TYPE

The choices are **STANDARD** (def) and **SPECIFIED**. The following standard UDP protocols are relayed when set: DHCP, TFTP, DNS, NTP (Network Time Protocol, port 123), NBNS (NetBios Name Server, port 137), NBDG (NetBIOS Datagram, port 138), and BootP. When **SPECIFIED** is set, the UDP port (1 to 65535) can be specified in the UDP Port columns (up to three per server).

#### UDP PORT 1, 2, 3

Used for specifying UDP ports to be relayed. These fields only apply when **UDP PORT TYPE** is set to **SPECIFIED**. Default is **0**.

### ROUTER > STATUS

View the **IP ROUTES**, **IP STATS**, and **ARP CACHE** statistics from this menu.

### ROUTER > STATUS > IP ROUTES

This lists the contents of the unit's IP route table.

### ROUTER > STATUS > IP ROUTES > IP ADDRESS

Network or host destination address.

### ROUTER > STATUS > IP ROUTES > NETMASK

Network mask applied to the destination address.

### ROUTER > STATUS > IP ROUTES > GATEWAY

Host or router to receive this packet.

### ROUTER > STATUS > IP ROUTES > PORT

Port gateway is located on:

| | |
|---|---|
| **LOCAL** | Sent directly to the unit's router |
| **ETH0** | The unit's Ethernet port |
| **WAN0** | The unit's first PPP bundle |
| **FR 0 . . . FR 9** | The unit is connected up to 10 DLCIs |

### ROUTER > STATUS > IP ROUTES > USE

Number of times the unit has referenced the route.

### ROUTER > STATUS > IP ROUTES > FLAGS

Important tags associated with this route entry

| | |
|---|---|
| **H** | route is a host route |
| **G** | route is a gateway route |
| **S** | static route, or learned via IPCP, IARP, DHCP |
| **R1** | learned from RIP Version 1 |
| **R2** | learned from RIP Version 2 |
| **I** | route learned from an ICMP redirect |
| **C** | directly connected interface |
| **P** | route is private and is not advertised with RIP |
| **T** | route is to a triggered port (updates only when table changes) |
| **U** | learned by unknown method |

### ROUTER > STATUS > IP ROUTES > HOPS

Number of routers that must go through to get to destination. Ranges from 0-15 or 16 for infinite (can't get there from here).

## ROUTER > STATUS > IP ROUTES > TTL

Seconds until address is removed from table. Value of 999 means route is static.

## ROUTER > STATUS > IP STATS

This section describes the following **STATISTICS** submenus (and see the tables on the pages following):

- IP
- ICMP
- TCP
- UDP

All of these statistics are taken from the MIB-II variables in RFC 1156. To clear the accumulated statistics, press the **<ENTER>** key on **CLEAR COUNTS**.

## ROUTER > STATUS > IP STATS > IP

View the IP statistics from this menu.

### DEFAULT TTL

The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this unit, whenever a TTL value is not supplied by the transport layer protocol.

### IP DATAGRAMS RECEIVED

The total number of input datagrams received from interfaces, including those received in error.

### BAD HEADER PACKETS

The number of input datagrams discarded due to errors in their IP headers, including bad check sums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

### BAD IP ADDRESSES

The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this unit. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

### TOTAL FORWARDED DATAGRAMS

The number of input datagrams for which this unit was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this unit, and the Source-Route option processing was successful.

### BAD PROTOCOL DISCARDS

The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

### DATAGRAMS DISCARDED

The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

### SENT DATAGRAMS TO UPPER LAYERS

The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

### IP DATAGRAMS SENT

IP packets from the unit's IP stack.

### ERRORFREE DISCARDS

The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in **TOTAL FORWARDED DATAGRAMS** if any such packets met this (discretionary) discard criterion.

### ROUTELESS DISCARDS

The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in **TOTAL FORWARDED DATAGRAMS** which meet this “no-route” criterion. Note also that this includes any datagrams which a host cannot route because all of its default gateways are down.

### IP REASSEMBLY TIMEOUT

The maximum number of seconds received fragments are held while awaiting reassembly at this unit.

### DISASSEMBLED FRAGMENTS

The number of IP fragments received which needed to be reassembled at this unit.

### IP DATAGRAMS REASSEMBLED

The number of IP datagrams successfully reassembled.

### IP REASSEMBLY FAILURES

The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably RFC 815s) can lose track of the number of fragments by combining them as they are received.

### SUCCESSFUL FRAGMENTS

The number of IP datagrams that have been successfully fragmented at this unit.

### FAILED FRAGMENTS

The number of IP datagrams that have been discarded because they needed to be fragmented at this unit but could not be e.g., because their “Don't Fragment” flag was set.

### TOTAL IP FRAGMENTS

The number of IP datagram fragments that have been generated as a result of fragmentation at this unit.

### DISCARDED ROUTING ENTRIES

A packet the unit couldn't route.

### CLEAR COUNTS

Setting this activator clears the IP Statistics.

## ROUTER > STATUS > IP STATS > ICMP

### ICMP MESSAGES RECEIVED

The total number of ICMP messages the unit received. Note that this counter includes all those counted by **ICMP SPECIFIC ERRORS**.

### ICMP SPECIFIC ERRORS

The number of ICMP messages the unit received but determined as having errors (bad ICMP checksums, bad length, etc.)

### ICMP DEST. UNREACHABLE MSGS RCVD

The number of ICMP Destination Unreachable messages received.

### ICMP TIMEOUTS RECEIVED

The number of ICMP Time Exceeded messages received.

### ICMP PARAMETER PROBLEM MSGS RCVD

The number of ICMP Parameter Problem messages received.

### ICMP SOURCE QUENCH MSGS RCVD

The number of ICMP Source Quench messages received.

### ICMP REDIRECTED MESSAGES RCVD

The number of ICMP Redirect messages received.

### ICMP ECHO REQUEST MSGS RCVD

The number of ICMP Echo (request) messages received.

### ICMP ECHO REPLY MSGS RCVD

The number of ICMP Echo Reply messages received.

### ICMP TIMESTAMP REQUEST MSGS RCVD

The number of ICMP Timestamp request messages received.

### ICMP TIMESTAMP REPLY MSGS RCVD

The number of ICMP Timestamp Reply messages received.

### ICMP ADDRESS MASK REQUEST MSGS RCVD

The number of ICMP Address Mask Request messages received.

### ICMP ADDRESS MASK REPLY MSGS RCVD

The number of ICMP Address Mask Reply messages received.

### ICMP MESSAGES SENT

The total number of ICMP messages this unit attempted to send. Note that this counter includes all those counted by **ICMP PACKET ERRORS.**

### ICMP PACKET ERRORS

this unit did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.

### ICMP Dest. Unreachable Msgs Sent

The number of ICMP Destination Unreachable messages sent.

### ICMP Time Eceeded Msgs Sent

The number of ICMP Time Exceeded messages sent.

### ICMP Parameter Problem Msgs Sent

The number of ICMP Parameter Problem messages sent.

### ICMP Source Quench Msgs Sent

The number of ICMP Source Quench messages sent.

### ICMP Redirect Msgs Sent

The number of ICMP Redirect messages sent.

### ICMP Echo Request Msgs Sent

The number of ICMP Echo Request messages sent.

### ICMP Echo Reply Msgs Sent

The number of ICMP Echo Reply messages sent.

### ICMP Timestamp Request Msgs Sent

The number of ICMP Timestamp (request) messages sent.

### ICMP Timestamp Reply Msgs Sent

The number of ICMP Timestamp Reply messages sent.

### ICMP Addr Mask Request Msgs Sent

The number of ICMP Address Mask Request messages sent.

### ICMP Addr Mask Reply Msgs Sent

The number of ICMP Address Mask Reply messages sent.

### Clear Counts

Selecting this activator will clear the ICMP statistics.

## Router > Status > IP Stats > UDP

View the UDP statistics from this menu.

### UDP Datagrams Received

The total number of UDP datagrams delivered to UDP users.

### No Application at Dest. Port

The total number of received UDP datagrams for which there was no application at the destination port.

### UDP Bad Packets

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

### UDP Datagrams Sent

The total number of UDP datagrams sent from this unit.

### Clear Counts

Selecting this activator clears the UDP statistics.

## Router > Status > IP Stats > UDP Table

View the UDP table statistics from this menu.

### Local IP Address

The destination IP address of the packet

### Port

The destination UDP port of the packet.

## Router > Status > IP Stats > TCP

View the TCP statistics from this menu.

### Retransmission Timeout Algorithm

The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.

### MIN RETRANSMISSION TIMEOUT (MS)

The minimum value permitted by a **TCP** implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the **LBOUND** quantity described in RFC 793.

### MAX RETRANSMISSION TIMEOUT (MS)

The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the **UNBOUND** quantity described in RFC 793.

### MAX TCP CONNECTIONS

The limit on the total number of **TCP** connections the unit can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

### ACTIVE TCP CONNECTIONS

The number of times **TCP** connections have made a direct transition to the **SYN-SENT** state from the **CLOSED** state.

### TCP PASSIVE CONNECTIONS

The number of times **TCP** connections have made a direct transition to the **SYN-RCVD** state from the **LISTEN** state.

### TCP FAILED ATTEMPTS

The number of times **TCP** connections have made a direct transition to the **CLOSED** state from either the **SYN-SENT** state or the **SYN-RCVD** state, plus the number of times **TCP** connections have made a direct transition to the **LISTEN** state from the **SYN-RCVD** state.

### TOTAL TCP RESETS

The number of times TCP connections have made a direct transition to the **CLOSED** state from either the **ESTABLISHED** state or the **CLOSE-WAIT** state.

### TCP CURRENT CONNECTIONS

The number of TCP connections for which the current state is either **ESTABLISHED** or **CLOSE-WAIT**.

### TCP SEGMENTS RECEIVED

The total number of segments received, including those received in error. This count includes segments received on currently established connections.

#### TCP Segments Sent

The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

#### Total TCP Retransmits

The total number of segments retransmitted -- that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

#### Clear Counts

Selecting this activator clears the TCP statistics.

### Router > Status > IP Stats > TCP Conns

View the TCP Conns Statistics from this menu. This table shows the different states of each TCP connection.

#### State

The possible states are **Free**, **Closed**, **Listen**, **Sync Sent**, **Sync Received**, **Established**, **Finwait1**, **Finwait2**, **Closewait**, **Lastack**, **Closing**, and **Timewait**.

#### Local IP Address

Local IP address of the TCP connection.

#### Local Port

Local port of the TCP connection.

#### Remote IP Address

Remote IP address of the TCP connection.

#### Remote Port

Remote port of the TPC connection.

### Router > Status > IP Stats > ARP Cache

This lists the contents of the units's ARP table. All resolved cache entries time out after 20 minutes. Unresolved entries time out in 3 minutes. The ARP cache can be cleared by pressing "**f**" while on the menu or by pressing "**d**" on the individual number for that entry.

### IP ADDRESS

IP address used for resolving MAC address.

### MAC ADDRESS

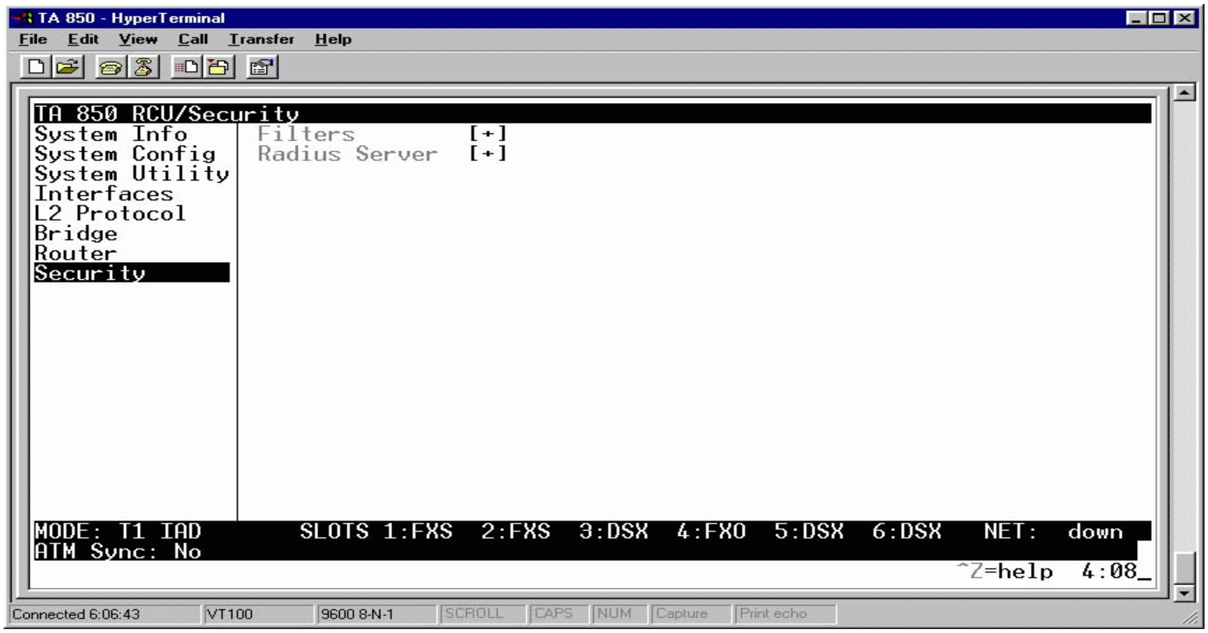
Ethernet address resolved (0=no resolution).

### TIME

Minutes since entry was first entered.

## SECURITY

Configure the **SECURITY FILTERS** and **RADIUS SERVER** parameters from this menu as shown in Figure 9.



```
TA 850 RCU/Security
System Info      Filters          [+]
System Config    Radius Server    [+]
System Utility
Interfaces
L2 Protocol
Bridge
Router
Security

MODE: T1 IAD        SLOTS 1:FXS  2:FXS  3:DSX  4:FXO  5:DSX  6:DSX   NET:  down
ATM Sync: No
                                                          ^Z=help  4:08_
```

**Figure 9. Security Menu**

## SECURITY > FILTERS

Configure the filter characteristics from this menu.

## SECURITY > FILTERS > FILTER DEFINES

The unit can filter packets based on certain parameters within the packet. The method used by the unit allows the highest flexibility for defining filters and assigning them to a PVC or PPP link. The filters are set up in two steps: (1) defining the filter types, and (2) applying them to a list under the PVC or PPP configuration. This menu is used to define the individual filter defines based on packet type.

NOTE *The Filter Defines option works for Frame Relay and PPP.*

## SECURITY > FILTERS > FILTER DEFINES > MAC FILTER DEFINES

The MAC filter is applied to bridge packets only. Bridge packets which are forwarded by the bridge functionality of the unit are defined here. Up to 32 MAC defines can be specified.

### NUM

Indicates the entry number in the MAC Filter Defines table.

### NAME

Identifies the filter entry. Default is no entry in **NAME** field.

### SRC ADDR

48-bit MAC source address used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

### SRC MASK

Bits in the MAC source address which are compared. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

### DEST ADDR

48-bit MAC destination address used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

### DEST MASK

Bits in the MAC destination address used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

### TYPE

16-bit type field used for comparison. Values are in hexadecimal format. Default is **00:00**.

#### TYPE MASK

Bits in the type field used for comparison. Values are in hexadecimal format. Default is **00:00**.

### SECURITY > FILTERS > FILTER DEFINES > PATTERN FILTER DEFINES

The pattern filter is applied to bridge packets only. That is any packet which is forwarded by the bridge functionality of the unit. Up to 32 pattern defines can be specified.

#### NUM

Indicates the entry number in the Pattern Filter Defines table.

#### NAME

Identifies the filter entry. Default is no entry in **NAME** field.

#### OFFSET

Offset from beginning of packet of where to start the pattern comparison. Default is **0**.

#### PATTERN

64 bits used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00:00:00**.

#### MASK

Bits in the pattern to be compared. Values are in hexadecimal format. Default is **00:00:00:00:00:00:00:00**.

### SECURITY > FILTERS > FILTER DEFINES > IP FILTER DEFINES

The IP filter defines apply to any IP packet, whether it is routed or bridged. Up to 32 IP defines can be specified.

#### NUM

Indicates the entry number in the IP Filter Defines table.

#### NAME

Identifies the filter entry. Default is no entry in name field.

#### SRC ADDR

IP address compared to the source address. Value is in dotted decimal format. Default is **0.0.0.0**.

### SRC MASK

Bits which are used in the source comparison. Value is in dotted decimal format. Default is **0.0.0.0**.

### DEST ADDR

IP address compared to the destination address. Value is in dotted decimal format. Default is **0.0.0.0.**

### DEST MASK

Bits which are used in the destination comparison. Value is in dotted decimal format. Default is **0.0.0.0.**

### SRC PORT

IP source port number used for comparison. Value is in decimal format. Range: **0 TO 65535**. Default is **0**.

### SRC PORT COMP

Type of comparison that is performed. Default is **NONE**.

**=** means ports equal to

**NOT =** means port not equal to

**>** means port greater than

**<** means port less than

**None** - means the source port is not compared

### DEST PORT

IP destination port number used for comparison. Value is in decimal format. Range: **0 TO 65535**. Default is **0**.

### DEST PORT COMP

Type of comparison that is performed. Default is **NONE**.

**=** means ports equal to

**NOT =** means port not equal to

**>** means port greater than

**<** means port less than

**None** - means the source port is not compared

### PROTO PORT

Protocol used for comparison. Value is in decimal format. Range: **0 TO 255**. Default is **0**.

### PROTO PORT COMP

Type of comparison that is performed. Default is **NONE**.

**=** means ports equal to

**NOT =** means port not equal to

**>** means port greater than

**<** means port less than

**None** - means the source port is not compared

### TCP ESTAB

**Yes** - only when TCP established

**No** - only when TCP not established

**Ignore** - ignore TCP flags (default)

## SECURITY > RADIUS SERVER

The parameters for the **RADIUS SERVER** are configured in this menu.

NOTE *Telnet radius is only available in C.04 firmware or later.*

## SECURITY > RADIUS SERVER > SERVER 1

This is the IP address of the first **RADIUS SERVER** that the unit should attempt to communicate with when authenticating a telnet session. Default is **0.0.0.0.**

## SECURITY > RADIUS SERVER > SERVER 2

This is the IP address of the second **RADIUS SERVER** that the unit should attempt to communicate with when the primary server does not respond. Default is **0.0.0.0.**

## SECURITY > RADIUS SERVER > SERVER 3

This is the IP address of the third **RADIUS SERVER** that the unit should attempt to communicate with when authenticating a Telnet session. Default is **0.0.0.0.**

### SECURITY > RADIUS SERVER > UDP PORT

This is the UDP port the unit should use when communicating with the **RADIUS SERVER**. The default is **1812**, which is the commonly used port.

### SECURITY > RADIUS SERVER > SECRET

The **RADIUS SERVER** and unit share this text string. It is used by the **RADIUS SERVER** to authenticate the unit, the RADIUS client. The factory default is not to use a secret.

### SECURITY > RADIUS SERVER > RETRY COUNT (1-10)

The is the number of times the unit should send a request packet to the **RADIUS SERVER** without a response before giving up. If the number of attempts to communicate with the primary server is equal to the retry count, the second server (if defined) is tried. If the second server does not respond within the retry count the third sever (if defined) is tried. If the third server does not respond with the retry count, the Telnet session is not authenticated and is dropped. The default is **5**.

## Appendix A. Voice Gateway Quick Start Procedure (Voice Turn Up)

A typical VoATM application (see Figure 10) uses a Total Access 850 connected to an ATM network. For voice applications, a Voice Gateway is needed to interface with the PSTN. Jetstream, Tollbridge, CopperCom, and LES-CAS are popular Gateway types.

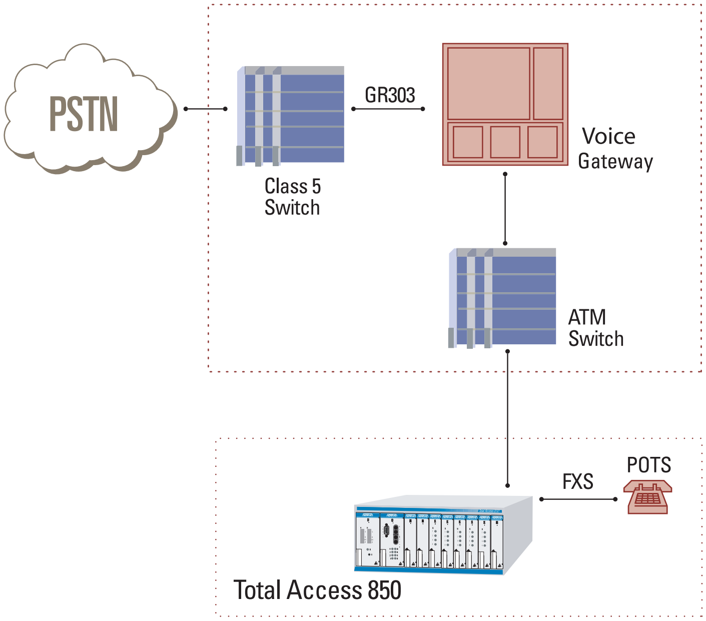


**Figure 10. Application Diagram**

To configure a Total Access 850 for use with the Voice Gateway, you need to know the VPI and VCI to be used on the ATM network to access the Gateway from this Total Access 850. You also need to know the format for **IDLE CELLS** and whether **DATA SCRAMBLING** is used on this ATM network. The following procedure will help you navigate the Total Access 850 menus for configuring the necessary elements for VoATM with the Voice Gateway.

To set the unit up for voice application, follow the steps below.

## *Setting up the T1 Interface*

**T1 Interface Setup Instructions**

| Step | Action |
|---|---|
| **1.** | From the main menu, select **INTERFACES**. |
| **2.** | Select **T1[0] CONFIG [+]** and press **<ENTER>**. |
| **3.** | Right arrow to select **FORMAT** and choose **ESF** or **SF**. |
| NOTE | *This format must match the format used by the other units in the network.* |
| **4.** | Set the Line Code to **B8ZS** or **AMI**. |
| NOTE | *This line code must match the line code used by the other units in the network.* |
| **5.** | Set the **EQUALIZATION** or line build out. The default setting of 0 dB is usually sufficient |
| **6.** | Set the **CSU LPBK** option to **ENABLE**, **DISABLE**, or **DISABLE ALL** based on whether looping to this unit from another unit will be allowed. |

## *Setting up the FXS Voice Ports*

**FXS Voice Ports Setup Instructions**

| Step | Action |
|---|---|
| **1.** | From the main menu, select **INTERFACES**. |
| **2.** | Select **FXS CONFIG [+]** and press **<ENTER>**. |
| **3.** | Set the **MODE** of each port to **LOOP START** or **GROUND START**. |
| NOTE | *This mode needs to be set based on how the network is set up and how each port is being used. Each port does not need to be set to the same mode.* |
| **4.** | Set the Line Code to **B8ZS** or **AMI**. |
| NOTE | *Set the* **TX (dB)** *or transmit direction level points of each port. Default is recommended,* |
| **5.** | Set the **RX (dB)** or receive direction level points of each port. Default is recommended. |
| **6.** | Set the **SVC MODE** of each port to either **IN SERVICE** or **OUT OF SVC**. |
| **7.** | Set the **LINE Z**, or line impedance, of each port based on the size of the network. Default is recommended. |
| **8.** | Set the **MSG IND** to **DISABLE** or **ENABLE**. When set to enable, talk path is always open, even in on-hook conditions, in order for FXS message tones to pass through. Disabling this feature will allow higher on-hook voltage but will not allow on-hook messaging other than caller ID. |

| Voice Turn Up | |
|---|---|
| **Step** | **Action** |
| **1.** | From the Total Access 850 main menu, select the **L2 PROTOCOL T1[0]** menu. (Here you set up the ATM network.) |
| **2.** | Under the main config [+] field, select the **ATM CONFIG** menu. |
| **3.** | Enter the **IDLE CELLS** format for your network. |
| **4.** | Set **DATA SCRAMBLING** appropriately for your network. |
| **5.** | Back all the way out to one level to the **PVC CONFIG** menu, and press **<ENTER>**. Enter the VPI and VCI values for communicating with that Gateway. (From this menu, the appropriate Voice information for working with the Voice Gateway is entered by selecting **VOICE** under the **CONNECTION** field.) |
| **6.** | Select **SETUP**, and from the **SETUP** menu, enter the Gateway type under **CALL CONTROL** and enter the VPI and VCI values for communicating with that Gateway.<br>For this application, **CALL CONTROL**, the **VPI** and **VCI** values should be set appropriately for your network. |
| **7.** | To verify correct setup, use the **PVC STATUS** menu (under the **STATUS** menu located at **L2 PROTOCOL [0] > STATUS**) to look at the current status of the voice connection.<br>Under **STATUS**, you can view information about the voice PVC along with information about the POTs ports available on the Gateway.<br>The **PROTOCOL STATUS** menu should show the Gateway Link is Active [Yes] (if everything is configured correctly). |

## Appendix B. RFC1483 Quick Start (IP Routing)

The Total Access 850 allows for complete integration of voice and data delivery from one compact platform (see Figure 11). Once you have completed the voice turn up procedure from the previous example, adding data to the circuit requires some additional setup.

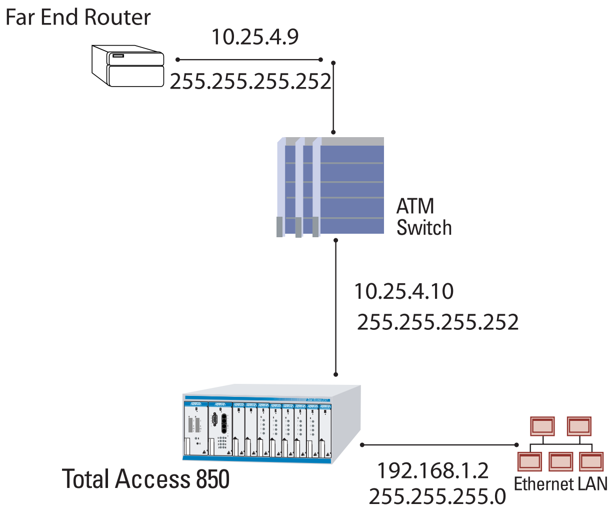


**Figure 11. Application Diagram**

To configure a Total Access 850 for IP routing, you need to know the VPI and VCI values for the data circuit on your network. You also need the IP address of the next hop router in the circuit.

The table on the next page shows how to configure the Total Access 850 for IP Routing.

.

**IP Routing**

| Step | Action |
|---|---|
| **1.** | From the Total Access 850 main menu, select the **L2 PROTOCOL > INTERFACES** menu. (Here you set up the ATM network.) |
| **2.** | Select the **ATM CONFIG** menu located under the main **CONFIG [+]** field. |
| **3.** | Enter the **IDLE CELLS** format for your network. |
| **4.** | Set **DATA SCRAMBLING** appropriately for your network. |
| **5.** | Back all the way out to the top level Total Access 850 menu, and then select the **ROUTER** menu. |
| **6.** | From the **CONFIG [+]** menu, you will set up addresses for your LAN and WAN.<br>For basic IP routing, use all the default values. |
| **7.** | Select the **INTERFACE > SETUP [+]** menu, enter the **IP** menu to enter your LAN configuration under **PRIMARY IP**. |
| **8.** | Enter your LAN **IP ADDRESS** and **SUBNET MASK** information.<br>For this example, the **IP ADDRESS** is 192.168.1.2, the **SUBNET MASK** is 255.255.255.0. Enter the Default Gateway under **ROUTER > CONFIG > ROUTES**. |
| **9.** | Arrow back to the main menu, and select the **L2 Protocol Interfaces** menu and then the **Config > PCV Config** menu. (Here you will enter your data PVC information.) |
| **10.** | Create a new PVC by entering the menu and press <i> under **NUM** field. Enter your VPI and VCI values. |
| **11.** | From the **Main Router > Config > Interfaces (T1[0]) > Setup** menu, enter your LAN information.<br>For this example, the **FAR END IP ADDRESS** is 10.25.4.9, the **IP NETMASK** is 255.255.255.252, and the **LOCAL IP ADDRESS** is 10.25.4.10. |
| **12.** | Arrow back to the top level Total Access 850 menu to activate your changes. |

## Appendix C. RFC1483 Quick Start (IP Routing with NAT)

To illustrate the use of NAT, consider the example from Appendix B. To set up a single public address that will be used to access the public network, you will use the **NAT** menu.

| IP Routing with NAT | |
|---|---|
| **Step** | **Action** |
| **1.** | The NAT menu is found under **TA 850/RCU/ROUTER/CONFIGURATION/WAN/ATM/RFC 1483 IP/NAT**. |
| **2.** | From the **NAT** menu, set **NETWORK ADDRESS TRANSLATION** to **ENABLED**. (This will enable translation and populate the corresponding NAT menu options.) |
| **3.** | Set **PUBLIC IP ADDRESS MODE** to either **INTERFACE** or **SPECIFIED**.<br>• **INTERFACE** is the default and will use the WAN IP address for the NAPT address.<br>• **SPECIFIED** allows you to enter another public address for private addresses to be translated into.<br>For basic NAT, this is all of the configuration that needs to be done.<br>For specific port translations or 1:1 mapping, you can enter **TRANSLATION TABLE** [+]. |
| **4.** | From the **TRANSLATION TABLE** menu, create a new entry by using the right arrow to enter the table. |
| **5.** | Create specific NAT translations based on your application.<br>**PUBLIC IP ADDRESS MODE SPECIFIED** Choice of using the NAPT address or specifying a different public address to be used for this translation.<br>**PROTOCOL MODE** Protocol for this translation. (TCP, UCP, ICMP, TCP or UDP, TCP UDP or ICMP, All, Specified, and NONE.)<br>**PRIVATE ADDRESS MODE** **SPECIFIED** or **ANY INTERNAL**. Choosing **SPECIFIED** brings up the **PRIVATE ADDRESS** option.<br>**TRANSLATE BODY** **YES** or **NO**. If set to **YES**, this will translate the body of the data packet and replace the private address with the NAPT address. Default is **NO**, which is used for most applications. |

## Appendix D. RFC 1483 Quick Start (Bridging)

The Total Access 850 allows for complete integration of voice and data delivery from one compact platform. Once you have completed the voice turn up procedure from the previous example, adding data to the circuit requires some additional setup.

To configure a Total Access 850 for Bridging, you need to know the VPI values for the data circuit on your network.

| Bridging | |
|---|---|
| **Step** | **Action** |
| **1.** | From the Total Access 850 main menu, select the **L2 PROTOCOL > INTERFACES** menu. (Here you set up the ATM network.) |
| **2.** | Select the **ATM CONFIG** menu located under the main **CONFIG [+]** field. |
| **3.** | Enter the **IDLE CELLS** format for your network. |
| **4.** | Set **DATA SCRAMBLING** appropriately for your network. |
| **5.** | Back all the way out to the top level Total Access 850 menu, and then select the **CONFIG [+]** for the **ETH [1]** menu. |
| **6.** | From the **CONFIG [+]** menu, you will set the **MODE** to **BRIDGE ALL**. |
| **7.** | Select the **INTERFACE > SETUP [+]** menu, enter your LAN configuration under **PRIMARY IP**. |
| **8.** | Enter your LAN **IP ADDRESS** and **SUBNET MASK** information.<br>For this example, the **IP ADDRESS** is 192.168.1.2, the **SUBNET MASK** is 255.255.255.0. |
| **9.** | Arrow back to the main menu, and select the **L2 Protocol Interfaces** menu and then the **Config > PCV Config** menu. (Here you will enter your data PVC information.) |
| **10.** | Create a new PVC by entering the menu and press <i> under **NUM** field. Enter your VPI and VCI values. |
| **11.** | Arrow back to the top level Total Access 850 menu to activate your changes. |

# SECTION 4.3 SDSL RCU USER INTERFACE GUIDE

This section of the Total Access 850 System Manual is designed for use by network administrators and others who will configure and provision the system. It contains SDSL RCU Module overview information, configuration information, and menu descriptions.

## CONTENTS

## FIGURES

## TABLES

## 1. SDSL RCU MODULE OVERVIEW

The SDSL Router Control Unit is a dual board assembly that includes an SDSL network interface, Nx56/64 V.35 interface, and built-in IP router. The SDSL RCU can provision, test, and provide status for any card in the channel bank. The faceplate has a DB-9 **CRAFT** port connection, and network, V.35, and Ethernet LEDs.

The SDSL RCU is only used in ATM applications. It supports vendor-specific SDSL protocols, ATM, and CopperMountain Frame Relay. Therefore, the SDSL RCU can interoperate with a variety of DSLAMs, including Lucent, Nortel, Copper Mountain, Nokia, and Alcatel. It also supports CopperCom, Jetstream, and Tollbridge Voice Gateways.

The SDSL RCU has built-in Echo Cancellation for up to 24 voice ports. Adaptive Differential Pulse Code Modulation (ADPCM) resources are also built-in for up to 24 ports.

To update firmware for the SDSL RCU, use XMODEM transfer protocol via the base unit's **CRAFT** port or use TFTP from a network server.

NOTE *Only the first two dipswitches on the RCU are used. With the first dip switch up (to the right of the unit if you are facing it), the unit boots up in a mode to update the firmware. With the second dip switch up, the unit factory defaults at startup.*

WARNING *SDSL firmware will not load on a T1 TDM RCU or T1 ATM RCU. The SDSL RCU (P/N 1200377L1) must be used for SDSL applications.*

The terminal menu is the access point to all other operations. Each terminal menu item has several functions and submenus that identify and provide access to specific operations and parameters. These menu selections are described later in this User Interface Guide.

## 2. VOICE OVER DSL OVERVIEW

Voice over DSL (VoDSL) refers to providing toll quality voice access to the Public Switched Telephone Network (PSTN) over twisted copper pair using DSL. Data can be combined with multiple voice lines over a single medium via DSL, thus yielding many advantages over traditional TDM technologies.

Traditional TDM technologies are limited by statically allocating bandwidth. DSL overcomes this by providing a large bandwidth and utilizing other technologies, such as ATM, to dynamically assign bandwidth as it is needed. Because of this, the user is able to add voice and data connections over a DSL line with flexibility and ease.

## 3. VOICE OVER ATM OVERVIEW

Voice over ATM is the technology used to transmit voice conversations over a data network using Asynchronous Transfer Mode (ATM). There are several potential benefits to moving voice over a data network using ATM. First, the small, fixed-length cells require lower processing overhead. Second, these small, fixed-length cells allow higher transmission speeds than traditional packet switching methods.

ATM allocates bandwidth on demand, making it suitable for high-speed connection of voice, data, and video services. Conventional networks carry data in a synchronous manner. Because empty slots are circulating even when the link is not needed, network capacity is wasted. ATM automatically adjusts the network capacity to meet the system needs.

## 4. VOICE OVER DSL APPLICATION

The Total Access 850 connects to a DSLAM via DSL and ATM. The SDSL RCU has a built in Echo Canceller that provides G.168 echo cancellation. The module can automatically detect ADPCM and enable it as needed.

Figure 1 shows a typical VoDSL application. The Total Access 850 connects to the ATM network, via a DSLAM, to provide both voice and high speed data from a single platform.

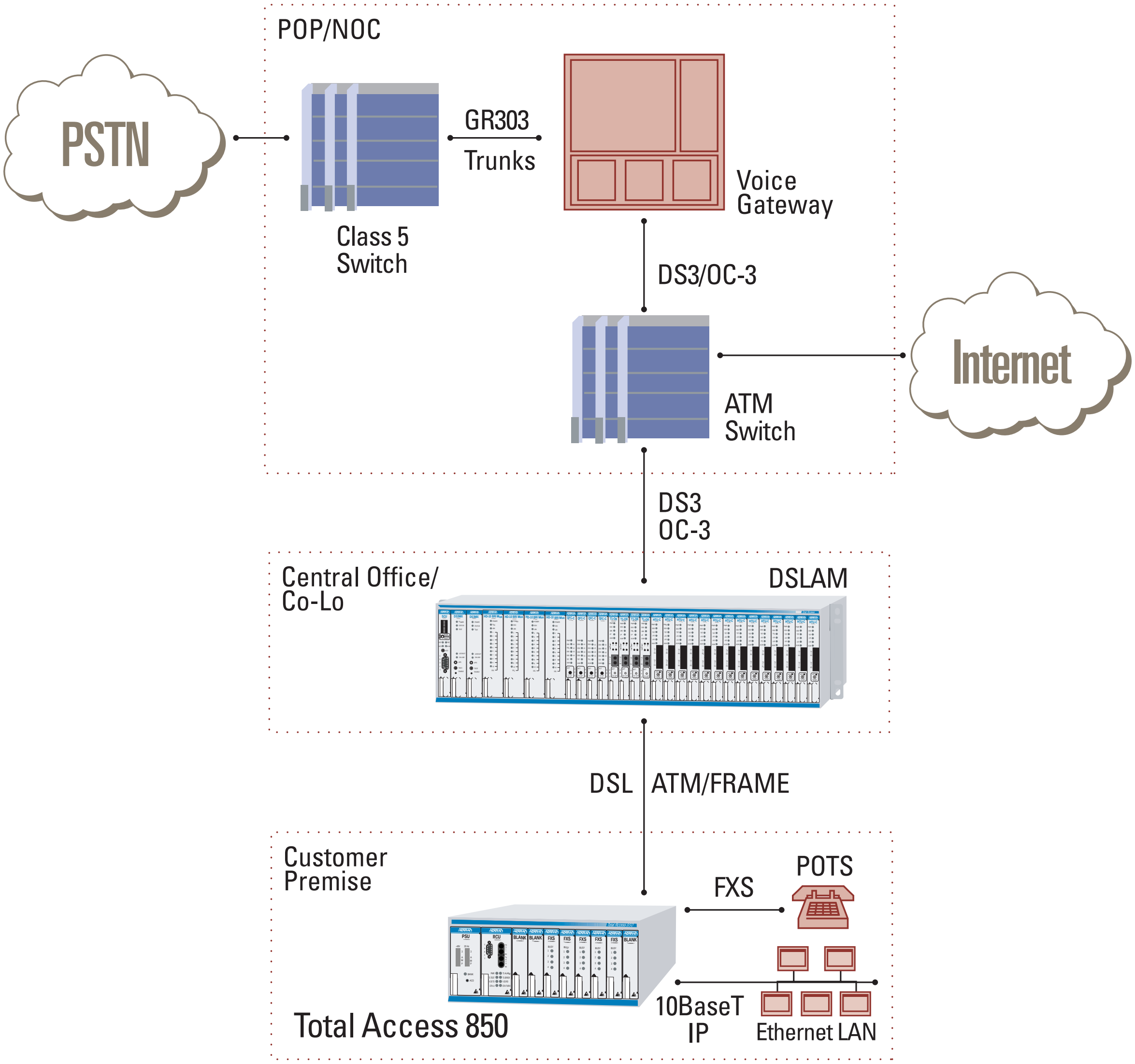
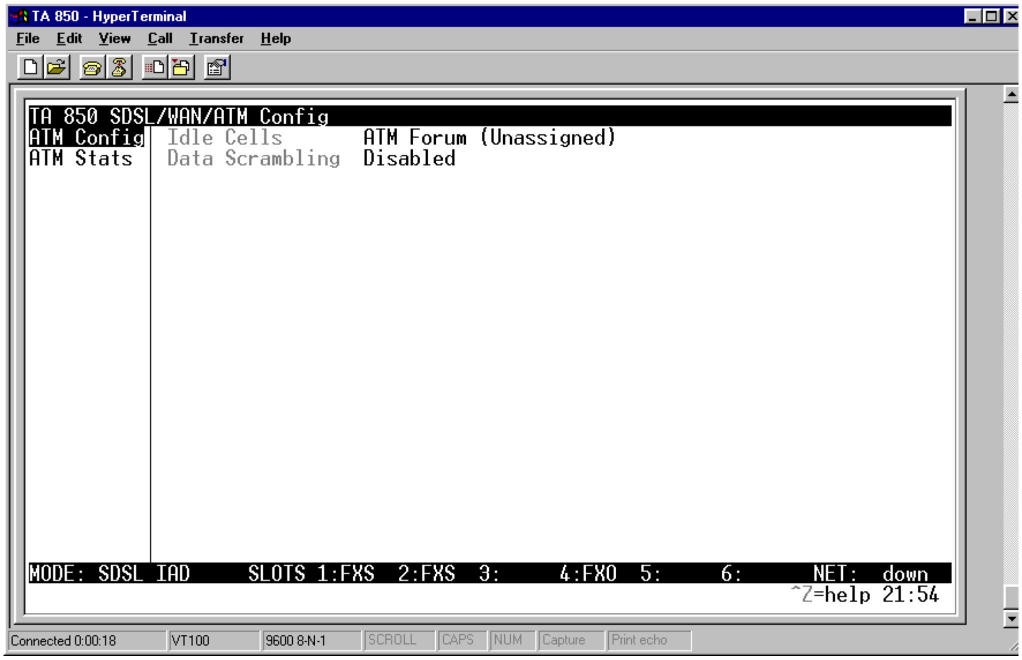


**Figure 1. Voice over DSL**

# 5. CONFIGURING THE TOTAL ACCESS 850

## System Info

The **SYSTEM INFO** menu provides basic information about the unit as well as data fields for editing information. Figure 2 displays the submenus that are available when you select this menu item.



```
TA 850 SDSL/WAN/ATM Config
ATM Config  Idle Cells        ATM Forum (Unassigned)
ATM Stats   Data Scrambling   Disabled

MODE: SDSL IAD     SLOTS 1:FXS  2:FXS  3:      4:FXO  5:      6:       NET:  down
                                                                ^Z=help 21:54
```

**Figure 2. System Information Menu**

### *>System Name*

Provides a user-configurable text string for the name of the Total Access 850. This name can help you distinguish between different installations. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an underbar). This name will appear on the top line of all screens.

### *>System Location*

Provides a user-configurable text string for the location of the Total Access 850. This field is to help you keep track of the actual physical location of the unit. You can enter up to 31 alphanumeric characters in this field, including spaces and special characters (such as an underbar).

### *>System Contact*

Provides a user-configurable text string for a contact name. You can use this field to enter the name, phone number, or email address of a person responsible for the Total Access 850 system. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an underbar).

### *>Unit Name*

Product-specific name for the controller card.

### >CLEI Code

The CLEI code for the controller card.

### > Part Number

ADTRAN part number for the controller card.

### >Serial Number

Serial number of the controller card.

### >Firmware Revision

Displays the current firmware revision level of the controller.

### >Bootcode Revision

Displays the bootcode revision.

### >System Uptime

Displays the length of time since the Total Access 850 system reboot.

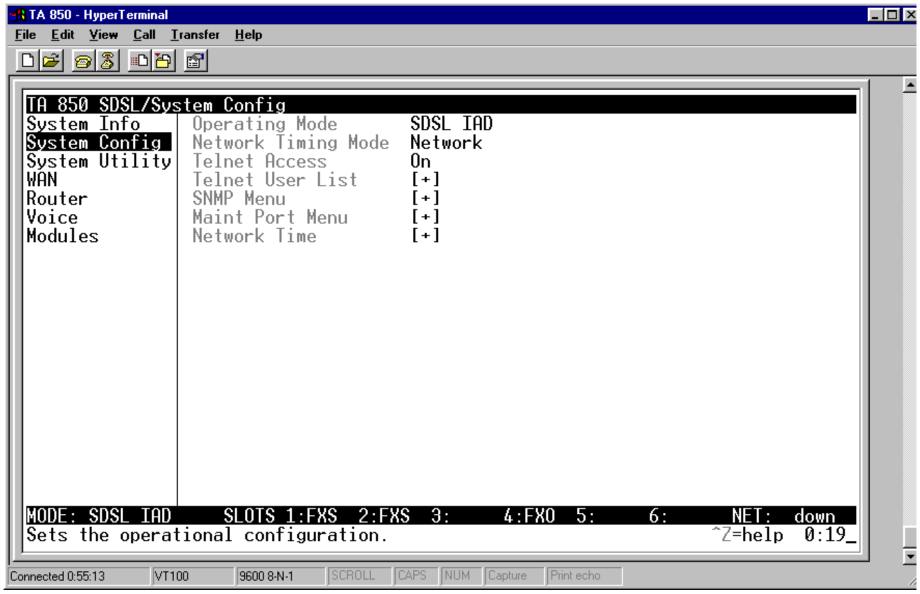
### >Date/Time

Displays the current date and time, including seconds. This field can be edited. Enter the time in 24-hour format (such as 23:00:00 for 11:00 pm). Enter the date in mm-dd-yyyy format (for example, 10-30-1998).

NOTE *Each time you reset the system, this value resets to 0 days, 0 hours, 0 min and 0 secs.*

## System Config

Set up the Total Access 850 operational configuration from the **SYSTEM CONFIG** menu. Figure 3 shows the items included in this menu.



```
TA 850 SDSL/System Config
System Info     Operating Mode        SDSL IAD
System Config   Network Timing Mode   Network
System Utility  Telnet Access         On
WAN             Telnet User List      [+]
Router          SNMP Menu             [+]
Voice           Maint Port Menu       [+]
Modules         Network Time          [+]

MODE: SDSL IAD     SLOTS 1:FXS  2:FXS  3:     4:FXO  5:      6:      NET:  down
Sets the operational configuration.                              ^Z=help  0:19_
```

**Figure 3. System Configuration Menu**

### *>Operating Mode*

The Total Access 850 can support various applications. For the SDSL RCU, **OPERATING MODE** will say **SDSL IAD**.

### *>Network Timing Mode*

The Total Access 850 supports **NETWORK** or **INTERNAL** timing. Default is **NETWORK.**

### *>Telnet Access*

Sets Telnet access to **ON** or **OFF**.

### *>Telnet User List*

Up to four users can be configured for access to the Total Access 850. Each user can be assigned a security level and time out.

**Name**

A text string of the user name for this session.

**Authen Method**

The user can be authenticated in two ways:

| | |
|---|---|
| **Password** | The Password field is used to authenticate the user. |
| **Radius** | The Radius client is used for authenticating the user. |

**Password**

When the authenticating method is password, this text string is used for the password.

**Idle Time (1-255)**

This sets the amount of time (in minutes) you can be idle before you are automatically logged off.

**Level**

This is the security level granted to the user (only levels 0-5). See the table below.

**Table 1. Password Security Level**

| Security Level | Description |
|---|---|
| **5** | Read-only permission for all menu items - **minimum rights** |
| **4** | Read permission for all menu items and permission to use test commands |
| **3** | Access to all commands except passwords, flash download, authentication methods, interface configurations, and telnet security levels |
| **2** | Access to all commands except passwords, flash download, authentication methods, and telnet security levels |
| **1** | Access to all commands except passwords and telnet security levels |
| **0** | Permission to edit every menu item, including creating and editing passwords - **maximum rights** |

### *>SNMP Menu*

The Total Access 850 is an SNMP agent. It can respond to Gets and Sets, and can generate traps. These two lists set up the manager, communities, and levels.

**Access**

When set to **OFF**, SNMP access is denied. When set to **ON** (def), the Total Access 850 will respond to SNMP managers based on the configuration.

**Communities**

This list is used to set up to eight SNMP communities names that the Total Access 850 will allow. Factory default sets the community “public” with **PRIVILEGES** set to **NONE**.

***Name***

This is a text string for the community name.

***Privilege***

The access for this manager can be assigned three levels.

| | |
|---|---|
| **None** | No access is allowed for this community or manager. |
| **Get** | Manager can only read items. |
| **Get/Set** | Manager can read and set items. |

***Manager IP***

This is the IP address of SNMP manager. If set to 0.0.0.0, any SNMP manager can access the Total Access 850 for this community.

**Traps**

The Total Access 850 can generate SNMP traps. This list allows up to four managers to be listed to receive traps.

***Manager Name***

This is the text string describing the name of the entry. It is intended for easy reference and has no bearing on the SNMP trap function.

***Manager IP***

This is the IP address of the manager that is to receive the traps.

### *>Maint Port Menu*

The Total Access 850's VT 100 **CRAFT** port can be accessed in two ways. One is a DB 9 located on the front, and the other is an RJ 48 located on the rear. The setup for these ports is under this menu. Only one of these access methods may be used at a time.

**Password Protect**

When set to **NO**, the maintenance port is not password protected. When **YES** (def), the Total Access 850 will prompt for a password upon startup.

**Password**

This is the text string that is used for comparison when password protecting the maintenance port. By default, no password is entered.

NOTE *The security level for the maintenance port is always set to 0. This gives full access to all menus.*

NOTE *Passwords are case-sensitive.*

**Instructions for Changing Passwords**

| Step | Action |
|---|---|
| **1.** | Select the **PASSWORD** field—a new **PASSWORD** field displays. |
| **2.** | Type the new password in the **ENTER** field. |

| **Instructions for Changing Passwords** | |
|---|---|
| **Step** | **Action** |
| **3.** | Type the new password again in the **CONFIRM** field. |
| NOTE | *The password can contain up to 12 alphanumeric characters. You can also use spaces and special characters in the password.* |

**Baud Rate**

This is the asynchronous rate that the maintenance port will run. The possible values are 300, 1200, 2400, 4800, 9600 (def)**,** 19200, 38400, 57600, and 115200.

**Data Bits**

This is the asynchronous bit rate that the maintenance port will run. The possible values are 7 or 8 (def) bits.

**Parity**

This is the asynchronous parity that the maintenance port will run. The possible values are **NONE** (def), **ODD,** or **EVEN**.

**Stop Bits**

This is the number of stop bits used for the maintenance port. The possible values are 1 (def), 1.5 or 2.

### *>Network Time*

The Total Access 850 unit time can be entered manually from the **SYSTEM INFO** menu, or the unit can receive time from an NTP/SNTP server. The **NETWORK TIME** menu includes all parameters relating to how the unit communicates with the time server.

**Server Type**

The server type defines the port on which the Total Access 850 will listen to receive timing information from the time server.

***NT Time***

The Total Access 850 will receive time from an NT server running SNTP software on its TIME port.

***SNTP***

The Total Access 8I50 will receive time directly from an SNTP server.

**Active**

This network timing feature can be turned on and off. It determines whether the unit will request and receive time from a time server.

**Time Zone**

There are several time zones available for which the time may be displayed. All time zones are based off of Greenwich Mean Time (GMT).

**Adjust for Daylight Saving**

Since some areas of the world use Daylight Savings Time, the Total Access 850 is designed to adjust the time on the first Sunday in April and the last Sunday in October accordingly if this option is turned on.

**Host Address**

This is the IP address of the time server that the Total Access 850 will request and receive time from.

**Refresh**

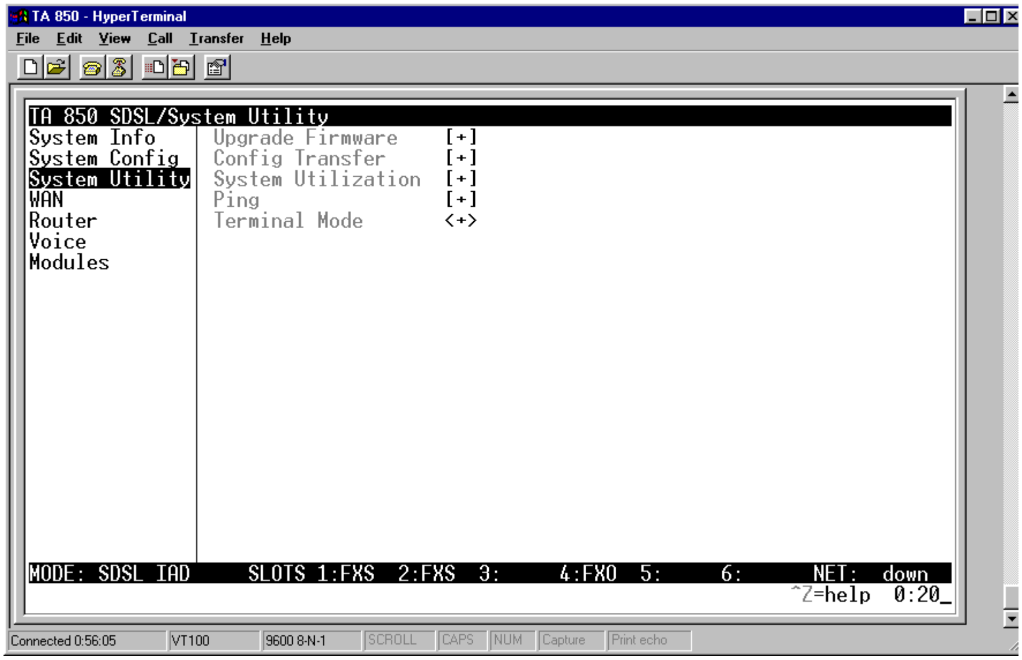
This is the interval of time between each request the Total Access 850 sends out to the time server. A smaller refresh time guarantees that the unit receives the correct time from the server and corrects possible errors more quickly. This may be more taxing on the machine. A range of refresh times is available for the user to decide which is best for their unit.

**Status**

This displays the current status of the time negotiation process. If an error is displayed, check all connections and configurations to try to resolve the problem.

## System Utility

Use the **SYSTEM UTILITY** menu to view and set the system parameters shown in Figure 4.



```
TA 850 SDSL/System Utility
System Info     Upgrade Firmware     [+]
System Config   Config Transfer      [+]
System Utility  System Utilization   [+]
WAN             Ping                 [+]
Router          Terminal Mode        <+>
Voice
Modules

MODE: SDSL IAD     SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET:  down
                                                              ^Z=help  0:20_
```

**Figure 4. System Utility Menu**

### *>Upgrade Firmware*

Updates firmware when Total Access 850 enhancements are released. Two transfer methods are available for use in updating the Total Access 850 system controller.

**Transfer Method**

The two methods for upgrading are **XMODEM** and **TFTP. TFTP** requires a TFTP server running somewhere on the network. The Total Access 850 starts a TFTP client function which gets the upgrade code from the TFTP server. Selecting **XMODEM** will load the upgrade code through the CRAFT port using any PC terminal emulator with xmodem capability.

**TFTP Server Address**

This is required when the transfer method is TFTP. It is the IP address or domain name (if DNS is configured) of the TFTP server.

**TFTP Server Filename**

This is required when the transfer method is TFTP. It is the case-sensitive file name which contains the upgrade code.

**Transfer Status**

This appears when TFTP is used. It displays the status of the transfer as it happens. Any error or success message will be displayed here.

**Start Transfer**

This activator is used when the configurable items in this menu are complete.

> *Before using* START TRANSFER*, the Total Access 850 should have a valid IP address, subnet mask, and default gateway (if required).*

**Abort Transfer**

Use this activator to cancel any TFTP transfer in progress.

### *>Config Transfer*

Sends a file containing the Total Access 850 configuration to a PC connected to the CRAFT port using XMODEM protocol or to a file on a TFTP server using the TFTP protocol.

CONFIG TRANSFER also lets you save the Total Access 850 configuration as a backup file, so you can use the same configuration with multiple Total Access 850 units. In addition, CONFIG TRANSFER can retrieve a configuration file from a TFTP server.

To support these transfers, ADTRAN delivers a TFTP program with the Total Access 850 called *TFTP Server*. You can configure any PC running Microsoft Windows with this software, and store a configuration file.

> *Before using* CONFIG TRANSFER*, the Total Access 850 should have a valid IP address, subnet mask, and default gateway (if required).*

Only one configuration transfer session (upload or download) can be active at a time.

**Transfer Method**
Displays the method used to transfer the configuration file to or from a server. XMODEM and TFTP are supported.

**Transfer Type**
Only **BINARY** transfers are currently supported.

**TFTP Server IP Address**
Specifies the IP address of the TFTP server. Get this number from your system administrator.

**TFTP Server Filename**
Defines the name of the configuration file that you transfer to or retrieve from the TFTP server. The default name is **ta850.cfg**, but you can edit this name.

**Current Transfer Status**
Indicates the current status of the update.

**Previous Transfer Status**
Indicates the status of the previous update.

**Load and Use Config**
Retrieves the configuration file specified in the **TFTP SERVER FILENAME** field from the server. To start this command, enter **Y** to begin or enter **N** to cancel.

CAUTION *If you execute this command, the Total Access 850 retrieves the configuration file, reboots, then restarts using the new configuration.*

**Save Config Remotely**
Saves the configuration file specified in **TFTP SERVER FILENAME** to the server identified in **TFTP SERVER IP ADDRESS**. To start this command, enter **Y** to begin or enter **N** to cancel.

CAUTION *Before using this command, you must have identified a valid TFTP server in **TFTP SERVER IP ADDRESS**.*

### *>System Utilization*

**Performance**
For internal use only.

**Queues**
For internal use only.

### >Ping

Allows you to send pings (ICMP requests) to hosts. The following items are under this menu:

> NOTE *Only one ping session can be active at a time.*

**Start/Stop**
Activator to start and cancel a ping test.

**Host Address**
IP address or domain name (if DNS is configured) of device to receive the ping.

**Size (40-1500)**
Total size of the ping to send. Range is 40 (def) to 1500 bytes.

**# of Packets**
Total packets to send every 2 seconds. Setting this to **0** allows the client to ping continuously.

**# Transmits**
Total packets sent (read only).

**# Receives**
Total packets received (read only).

**%Loss**
Percentage loss based on ping returned from host (read only).

### >Terminal Mode

The terminal mode gives the user the command-line prompt. From this prompt, you can:

- Perform a reset with the command “reset”
- Configure the unit. The Total Access 850 RCU can download a text file which contains the configuration of the entire unit. This configuration may then be altered in a text editor, and uploaded to that same or any other Total Access 850 RCU. See DLP-12 for further assistance.
- Debug and troubleshoot. This function would be carried out with the assistance of ADTRAN Technical Support at 888-423-8726.

## Configuring WAN Settings

### >DSLAM Type

Set this to the type of DSLAM the Total Access 850 will be connecting to. The Total Access 850 supports the Copper Mountain CE 150, ADTRAN Total Access 3000, Nokia D50, and Lucent Stinger DSLAMs.

### >Layer One Interface

This is the physical layer protocol used to connect the DSLAM to the Total Access 850.

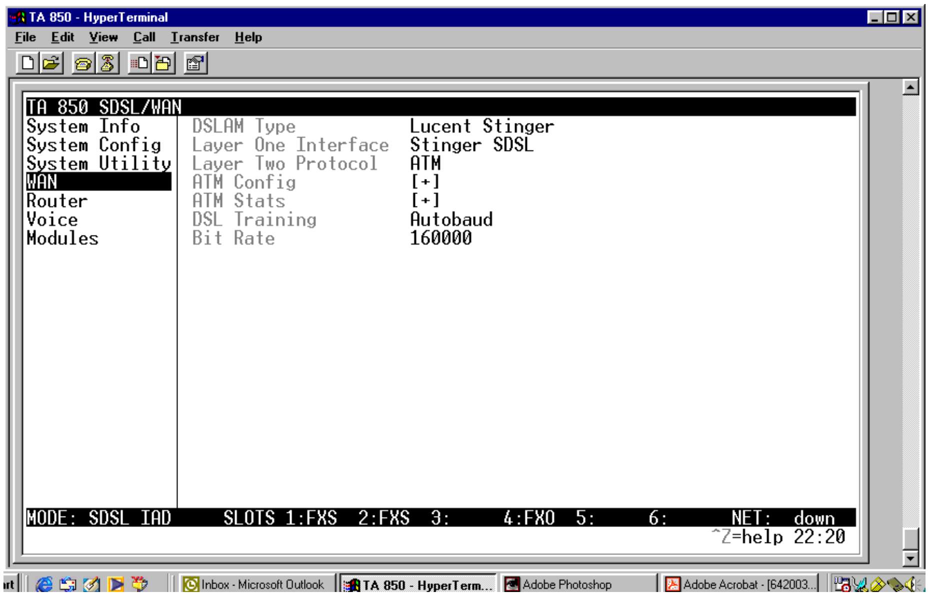
### >Layer Two Protocol

This is the data link layer protocol used to connect the DSLAM to the Total Access 850. This is selected appropriately for each DSLAM. The Layer 2 menus change according to this selection. If your DSLAM supports ATM, refer to *ATM Config* on page 256. For Frame Relay, refer to *Frame Relay* on page 257.

> NOTE
>
> *If the DSLAM Type is CopperMountain, refer to Appendix E. Routing in HDIA Mode on page 289 for information.*

### >ATM Config

Use the **WAN** menu (Figure 5) to access the **ATM CONFIG** menu.

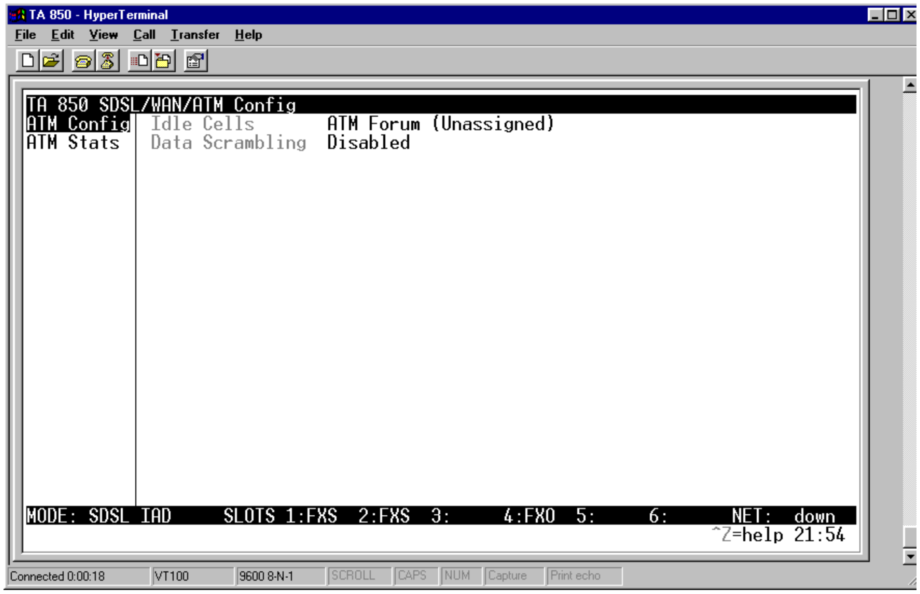

TA 850 - HyperTerminal
File Edit View Call Transfer Help
Inbox - Microsoft Outlook
TA 850 - HyperTerm...
Adobe Photoshop
Adobe Acrobat - [642003...

```
TA 850 SDSL/WAN
System Info      DSLAM Type              Lucent Stinger
System Config    Layer One Interface     Stinger SDSL
System Utility   Layer Two Protocol      ATM
WAN              ATM Config              [+]
Router           ATM Stats               [+]
Voice            DSL Training            Autobaud
Modules          Bit Rate                160000

MODE: SDSL IAD      SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:        NET:  down
                                                                  ^Z=help 22:20
```

**Figure 5. WAN Menu**

Use the **ATM CONFIG** menu (Figure 6) to set the parameters listed below the figure.



```
TA 850 SDSL/WAN/ATM Config
ATM Config   Idle Cells         ATM Forum (Unassigned)
ATM Stats    Data Scrambling    Disabled

MODE: SDSL IAD      SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:        NET:  down
                                                                    ^Z=help 21:54
```

**Figure 6. ATM Config Menu**

### Idle Cells

The **IDLE CELLS** format must be configured for either **ATM FORUM** or **ITU**. Configuring this setting incorrectly for a particular circuit will cause poor performance at the ATM layer.

NOTE *This setting must match the configuration setting of the ATM switch or DSLAM at the other end of the circuit.*

### Data Scrambling

**DATA SCRAMBLING** can be **ENABLED** or **DISABLED** for cell traffic. Configuring this setting incorrectly for a particular circuit will cause poor performance.

NOTE *This setting must match the configuration setting of the ATM switch or DSLAM at the other end of the circuit.*

## *>Frame Relay*

Frame Relay is a connection-oriented service requiring circuits to be configured by your carrier to establish a physical link between two or more locations. Multiple virtual circuits (which appear as virtual point-to-point links) can be run through the same physical connection.

There are two types of virtual circuits supported in Frame Relay: Permanent Virtual Circuits (PVC) and Switched Virtual Circuit (SVC). PVCs are like dedicated point-to-point private lines. Since the physical connection is always there in the form of a leased line, call setup and tear down is done by a carrier via a network management system. SVCs require setup and tear down and are generally not available from Frame Relay carriers. Virtually all Frame Relay communications are implemented using PVCs. The Total Access 850 supports PVCs only.

A number called the Data Link Connection Identifier (DLCI) identifies each virtual circuit within a shared physical channel.

**Frame Relay > Maintenance Protocol**

The Frame Relay maintenance protocol is used on the WAN port. The maintenance protocol is used to send link status and virtual circuit information between Frame Relay switches and other devices (such as routers) that communicate with them. Possible choices are listed below.

**ANNEX D (def)** This is an ANSI standard and is the most commonly used standard in the US.

**Annex A** This is the CCITT European standard.

**LMI** This was developed by a vendor consortium and is also known as the “consortium” management interface specification. It is still used by some carriers in the U.S.

**Static** This should be selected when there is no Frame Relay switch in the circuit. The DLCIs are assigned in the DLCI Mapping and must be the same for the device it will communicate with.

**Frame Relay > Polling Frequency**

This parameter is the interval that the Total Access 850 polls the Frame Relay switch using the maintenance protocol selected above. The Total Access 850 is required to poll the Frame Relay switch periodically to determine whether the link is active. The value is in seconds and ranges from 5 to 30 seconds with a default of 10 seconds.

**Frame Relay > DLCI Mapping**

This menu allows each DLCI to be mapped to a particular Frame Relay maintenance protocol. Each protocol parameter can be individually configured for each DLCI. By factory default, the DLCI map is empty.

When empty and a maintenance protocol other than static is used, the Total Access 850 will poll the switch to determine which DLCIs are active. These active DLCIs will attempt to determine the IP and IPX addresses on the other end of the virtual circuit using Inverse ARP (IARP). If there is a response, the network learned will be added to the router tables and the virtual circuit will be treated as an unnumbered interface. Bridge connections are made using bridge group 1.

When more than one DLCI mapping is listed, the Total Access 850 will try to match the DLCIs learned from the Frame Relay switch with the DLCI values in the map. If there is a match, the protocols specified in the map are used. However, if an active DLCI is not in the list, it looks for an entry that has 0 in the DLCI field. This entry is considered the default entry to use when no match occurs. If this default entry is not present, the Total Access 850 falls back to using IARP (as discussed in the previous paragraph) to determine the protocols to use with that particular virtual circuit. If a static maintenance protocol is used, at least one DLCI mapping must be specified.

*To insert a new profile, press the* **I** *key when over the* **NUM** *column. A new inserted profile will always be set up with the default parameters. To copy parameters from an old profile to this newly inserted profile, use the copy (***C***) and paste (***P***) keys. Entire configuration trees can be copied with this method.*

*To delete an unused profile, use the* **D** *key when the cursor is over the number in the* **NUM** *column. Once deleted, the profile is gone permanently as soon as the DLCI Mapping is saved. Items may be deleted when* **DEL** *appears below the status bar.*

***DLCI Mapping > Active***

When this parameter is set to **YES** (def), the mapping is used to determine the protocols used. If set to **NO**, the Total Access 850 will ignore the virtual circuit with this DLCI.

***DLCI Mapping > DLCI***

This is the DLCI associated with this virtual circuit. This value can range from 16 to 1007.

***DLCI Mapping > IP Map***

This menu represents the IP protocol mapping that is to take place for this DLCI.

***IP Map > Active***

When this is set to **YES** (def), the Total Access 850 will attempt to transport IP packets for this DLCI. A setting of **NO** means that no IP traffic or route will be exchanged.

***IP Map > IARP***

When this is set to **YES** (def), the Total Access 850 will send Inverse ARP packets to determine the IP address on the other end of the virtual circuit. If the IARP is responded to, a route is placed in the IP route table. A setting of **NO** means that the route address is to be assigned statically using the **IP MAP > FAR-END IP ADDRESS** parameter. The Total Access 850 will always respond to Inverse ARP requests.

***IP Map > Far-End IP Address***

This is the IP address of the device on the other end of the virtual circuit. When this DLCI becomes active, the Total Access 850 will add a route in the IP routing table.

***IP Map > IP Netmask***

The IP network mask to apply to the **FAR-END IP ADDRESS** and **LOCAL IP ADDRESS** is specified here.

***IP Map > Local IP Address***

The virtual circuit may require an IP address to be specified at this DLCI interface. This is called a numbered interface. This address is used by the Total Access 850 to respond to Inverse ARP requests. If this IP address is left as 0.0.0.0, the link is treated as unnumbered and the Total Access 850 responds to the Inverse ARP with its Ethernet IP address.

#### *IP Map > RIP*

**RIP > Version** The RIP protocol can be specified per DLCI. The possible selections are **OFF** (default) (meaning no RIP packets are listened to or sent), **V1** (which is RIP version 1) or **V2** (which is RIP version 2).

**RIP > Method** This specifies the way the RIP protocol sends out its advertisements.

**None (def)** All routes in the router table are advertised out this virtual circuit with no modification of the metrics.

**Split Horizon** Only routes not learned from this particular virtual circuit are advertised.

**Poison Reverse** All routes are advertised, but the routes learned from this port are “poisoned” with an infinite metric.

**RIP > Direction** This parameter specifies the direction at which RIP advertisements are sent and listened.

**Tx and Rx (def)** RIP advertisements are periodically transmitted and are listened to on this virtual circuit.

**Tx Only** RIP advertisements are periodically transmitted but are not listened to on this virtual circuit.

**Rx Only** RIP is not transmitted on this virtual circuit but they are listened to.

#### *IP Map > NAT*

The Total Access 850 can perform Network Address Translation over a PVC. Setting this option to **ON** will cause the Total Access 850 to translate between the Ethernet addresses and the configured **LOCAL IP ADDRESS**. Only one PVC may be used for translation at one time. If more than one IP Map is configured for NAT, the first PVC which is activated becomes the NAT port.

### *DLCI Mapping > IPX Map*

This menu represents the IPX protocol mapping that is to take place for this DLCI.

#### *IPX Map > Active*

When this is set to **YES**, the Total Access 850 will attempt to transport IPX packets for this DLCI. A setting of **NO** (def) means that no IPX traffic or route will be exchanged.

#### *IPX Map > IARP*

When this is set to **YES**, the Total Access 850 will send Inverse ARP packets to determine the IPX network on the other end of the virtual circuit. If the IARP is responded to, a route is placed in the IPX route table. A setting of **NO** (def) means that the IPX network is to be assigned to the link statically using the IPX Map/Link Network parameter. The Total Access 850 will always respond to Inverse ARP requests.

#### *IPX Map > Link Network*

This is the IPX network of the link or of the other device's LAN. When this DLCI becomes active, the Total Access 850 will add a route to this network in the IPX routing table. This address is also used by the Total Access 850 to respond to Inverse ARP requests. If this IPX address is left as 0, the link is treated as unnumbered and the Total Access 850 responds to the Inverse ARP with its Ethernet IPX address.

### *DLCI Mapping > Bridge Map*

This menu is used to permit bridging of packets over this DLCI. Each DLCI or virtual circuit must be assigned a bridge group. The bridge group treats all virtual circuits as one circuit. Bridge packets destined to be transmitted out a particular bridge group are copied and transmitted individually out each DLCI in the bridge group. However, incoming bridge packets received from one DLCI are not retransmitted out the other DLCIs in the same bridge group. Any device in the bridge group must transmit to each DLCI. This requires a fully meshed circuit, meaning each device has a virtual circuit to each other.

#### *Bridge Map > Active*

When this is set to **YES**, the Total Access 850 will bridge packets to and from this DLCI. Bridge packets are any packets that are not IP or IPX packets except when the router is turned off, in which case that particular router's protocol packets are bridged. A setting of **NO** (def) means that no bridging will occur.

#### *Bridge Map > Bridge Group*

The bridge group that this DLCI is part of is specified here as **GROUP 1** (def) or **GROUP 2**. These groups correspond to the spanning tree protocols Bridge Group 1 and Bridge Group 2.

### *DLCI Mapping > Filter*

The Total Access 850 can block packets in and out of a PVC port by use of the filters. They are set up in two steps: 1) define the types of packets that would be of interest in the **CONFIGURATION > SECURITY > FILTER DEFINES** menu, and 2) set up the filter type and combination of defines that will cause a packet block.

#### *Filter > In from PVC*

The packets which come into the Total Access 850 via this PVC can be filtered in three ways:

| | |
|---|---|
| **Disabled (def)** | Turns off packet input filtering. No incoming packets from this PVC are blocked. |
| **Block All** | All incoming packets from this PVC are blocked except as defined in the **FILTERS > IN EXCEPTIONS** list. |

| | |
|---|---|
| **Forward All** | All incoming packets from this PVC are not blocked except as defined in the **FILTERS > IN EXCEPTIONS** list. |

***Filter > In Exceptions***

This is a list of up to 32 filter entries which can be combined using the operations field. The operations are performed in the order they appear on the list.

| | | |
|---|---|---|
| **Active** | | Turns this entry active when set to **ON**. |
| **Type** | | Selects the filter define list to reference: |
| | **MAC** | from the **CONFIGURATION > SECURITY > FILTER DEFINES > MAC FILTER DEFINES** list. |
| | **Pattern** | from the **CONFIGURATION > SECURITY > FILTER DEFINES > PATTERN FILTER DEFINES** list. |
| | **IP** | from the **CONFIGURATION > SECURITY > FILTER DEFINES > IP FILTER DEFINES** list. |
| | **IPX** | from the **CONFIGURATION > SECURITY > FILTER DEFINES > IPX FILTER DEFINES** list. |
| **Filter List Name** | | Selects between filters defined in the list. |
| **Next Oper** | | The next operation to use to combine with the next filter in the list: |
| | **END** | the last filter to combination. |
| | **AND** | logically AND this filter with the next filter in the list |
| | **OR** | logically OR this filter with the next filter in the list. |

***Filter > Out to PVC***

The packets which transmit out this PVC from the Total Access 850 can be filtered in three ways:

| | |
|---|---|
| **DISABLED (def)** | Turns off packet output filtering. No outgoing packets to this PVC are blocked. |
| **Block All** | All outgoing packets to this PVC are blocked except as defined in the **FILTERS > OUT EXCEPTIONS** list. |
| **Forward All** | All outgoing packets to this PVC are not blocked except as defined in the **FILTERS > OUT EXCEPTIONS** list. |

***Filter > Out Exceptions***

This is a list of up to 32 filter entries. The setup is exactly the same as the **FILTER > IN EXCEPTIONS** list.

***Maintenance DLCI***

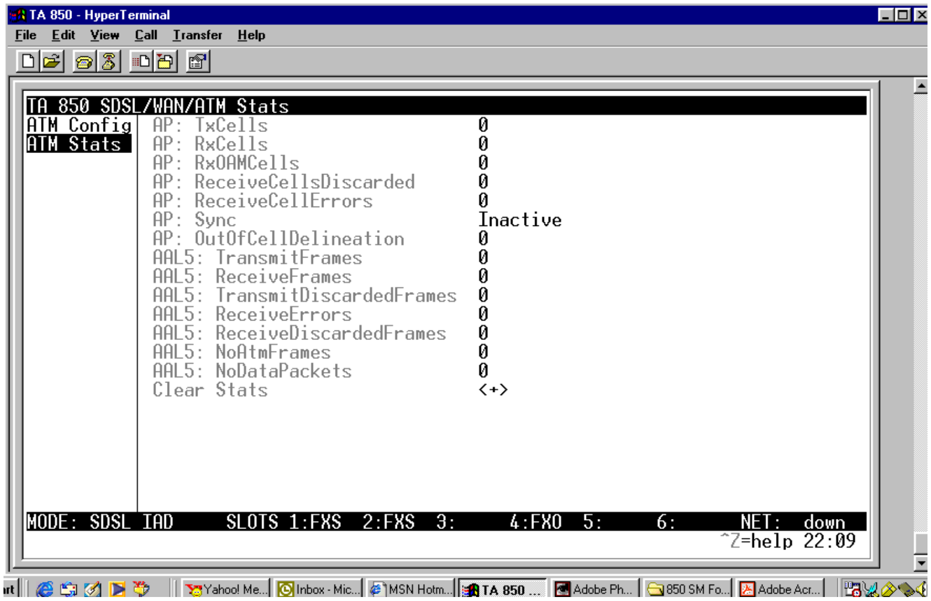
The Total Access 850 can be configured from the WAN without having to preset a DLCI mapping or IP address. This value is the DLCI number used to open an IP session by the Total Access 850. Any IP packet arriving from the PVC is assumed to be for the Total Access 850’s IP stack. The destination address in the packet is assigned as the PVC's local IP address. The source address is used to add a host route in the routing table. The default is 901, but any legal DLCI number can be used.

***BECN Timeout***

This value is expressed in milliseconds and represents the amount of time the Total Access 850 will stop transmitting over a PVC which received a packet with the BECN bit set. The default is 1.5 seconds.

## *>ATM Stats*

Use the **WAN** menu (Figure 5 on page 256) to access the **ATM STATS** menu (Figure 7) and view the parameters listed below the figure.



```
TA 850 SDSL/WAN/ATM Stats
ATM Config  AP: TxCells                    0
ATM Stats   AP: RxCells                    0
            AP: RxOAMCells                 0
            AP: ReceiveCellsDiscarded      0
            AP: ReceiveCellErrors          0
            AP: Sync                       Inactive
            AP: OutOfCellDelineation       0
            AAL5: TransmitFrames           0
            AAL5: ReceiveFrames            0
            AAL5: TransmitDiscardedFrames  0
            AAL5: ReceiveErrors            0
            AAL5: ReceiveDiscardedFrames   0
            AAL5: NoAtmFrames              0
            AAL5: NoDataPackets            0
            Clear Stats                    <+>

MODE: SDSL IAD     SLOTS 1:FXS  2:FXS  3:    4:FXO  5:    6:      NET:  down
                                                              ^Z=help 22:09
```

**Figure 7. ATM Stats Menu**

**AP: Tx Cells**

This is the number of cells transmitted.

**AP: Rx Cells**

This is the number of cells received.

**AP: Rx OAM Cells**

This is the number of OAM cells received

**AP: Receive Cells Discarded**

This is the number of cells received and discarded. An incrementing count in this field could indicate a configuration problem with the ATM layer.

**AP: Receive Cell Errors**

This is the number of cells received with an HEC error.

**AP: Sync**

This indicates cell delineation at the ATM layer.

**AP: Out Of Cell Delineation**
This indicates loss of cell delineation at the ATM layer.

**AAL5: Transmit Frames**
This is the number of AAL5 frames transmitted.

**AAL5: Receive Frames**
This is the number of AAL5 frames received.

**AAL5: Transmit Discarded Frames**
This is the number of AAL5 frames discarded.

**AAL5: Receive Errors**
This is the number of AAL5 errors received.

**AAL5: Receive Discarded Frames**
This is the number of AAL5 frames discarded.

**AAL5: No ATM Frames**
This is for internal use only.

**AAL5: No Data Packets**
This is for internal use only.

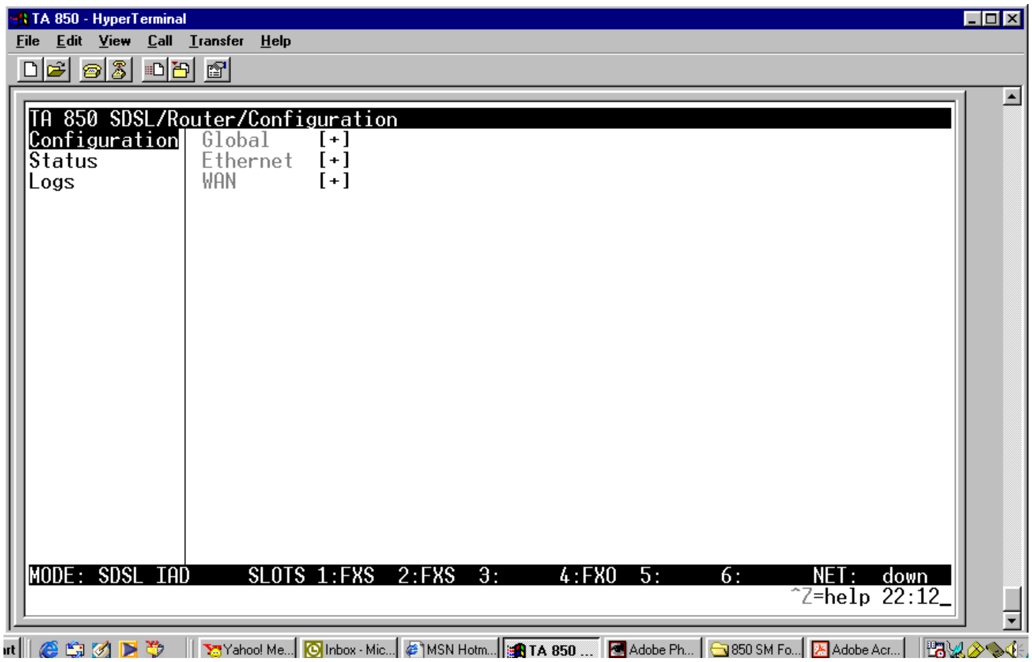
**Clear Stats**
This is used to clear the counters on this menu screen.

### *>DSL Rate Config*

The rate at which the SDSL link has trained is displayed here. If the selected DSLAM does not support Autobaud, then the line rate should be entered here.

## Configuring the Router – Configuration

Use the **ROUTER > CONFIGURATION** menu (Figure 8) to access the **GLOBAL**, **ETHERNET**, and **WAN** menus.



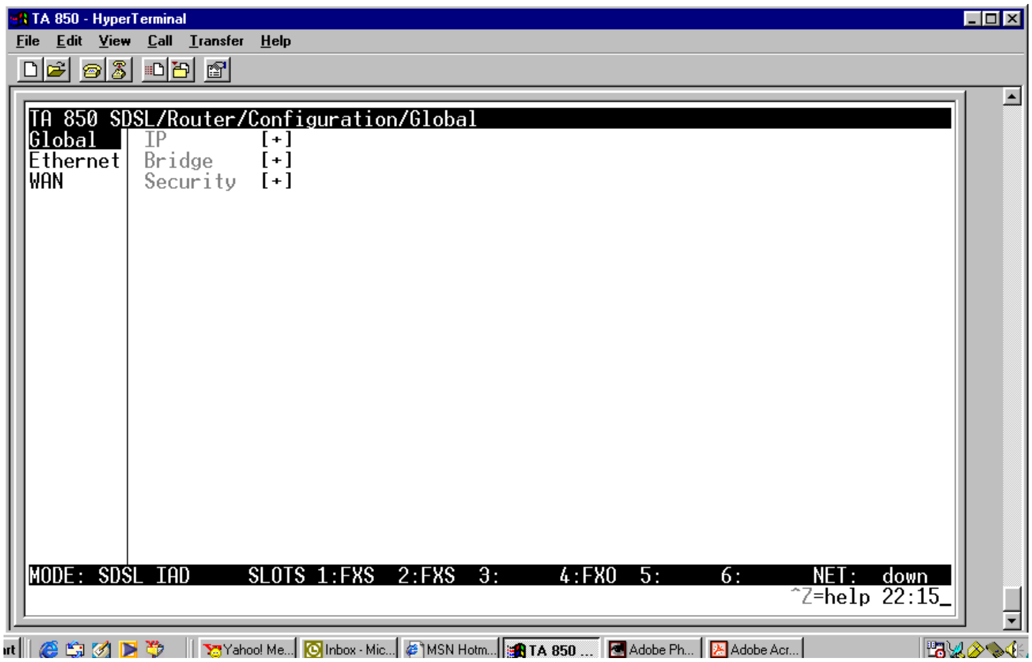
```
TA 850 SDSL/Router/Configuration
Configuration  Global    [+]
Status         Ethernet  [+]
Logs           WAN       [+]

MODE: SDSL IAD     SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET:  down
                                                              ^Z=help 22:12_
```

Figure 8. Router/Configuration Menu

### >Global

Use the GLOBAL menu (Figure 9) to set up general router functions.



```
TA 850 SDSL/Router/Configuration/Global
Global    IP        [+]
Ethernet  Bridge    [+]
WAN       Security  [+]

MODE: SDSL IAD     SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET:  down
                                                              ^Z=help 22:15_
```

Figure 9. Global Menu

### IP

This is used for general IP configuration.

#### *Mode*

This item controls how the 850 handles IP routes. When this option is set to **ON** (def), the 850 will advertise and listen to routes from other IP routers. If **OFF**, the route table is still used, but only static routes are used for routing IP packets and only the Ethernet port is used. IP packets can be sent over the WAN, but only when bridged.

#### *Static Routes*

Use this menu to enter static routes to other networks.

| | |
|---|---|
| **Active** | Adds this static route entry to the IP routing table when set to **YES** and removes it (if it was previously added) if set to **NO** (def). |
| **IP Address** | The IP address of the host or network address of the device being routed to. |
| **Subnet Mask** | Determines the bits in the previous IP address that are used. *If this is to be a host route, it must be set to  all ones* (255.255.255.255). |
| **Gateway** | The IP address of the router to receive the forwarded IP packet. |
| **HOPS** | The number of router hops required to get to the network or host. Maximum distance is 15 hops. |
| **Private** | When set to **NO**, the Total Access 850 will advertise this static route using RIP. Setting to **YES** means that the route is kept private. |

#### *DHCP Server*

| | |
|---|---|
| **DHCP Mode** | When set to **ON**, the Total Access 850 acts as a DHCP server and will dynamically assign IP, network mask, default gateway, and DNS addresses to any device which transmits a broadcast DHCP request. The addresses assigned are based on the Total Access 850's own IP address and will be within the same network. |
| **DHCP Renewal Time** | The number of hours that the DHCP server should allow the device before it is required to send a new DHCP request. The default is 15 hours, and 0 represents an infinite lease. |

#### *Domain Names*

Enter the 850's domain name and the primary and secondary DNS servers in this menu.

| | |
|---|---|
| **Domain Name** | Text string used to represent the domain name used by the Total Access 850. |
| **Primary DNS** | First server to which domain name requests are sent. |
| **Secondary DNS** | Server used as a backup, in case the primary address does not respond to the request. |
| **Primary NBNS/WINS** | Server to which NT domain name requests are sent. |
| **Secondary NBNS/WINS** | Server used when there is no response from the primary server. |

### *UDP Relay*

This menu configures the 850 to act as a UDP relay agent for applications requiring a response from UDP hosts that are not on the same network segment as their clients.

***Mode***

When this option is set to **ON**, the Total Access 850 will act as a relay agent.

***UDP Relay List***

Up to four relay destination servers can be specified in this list.

**Relay Address** This is the IP address of the server that will receive the relay packet.

**UDP Port Type**

**STANDARD (def)** The following standard UDP protocols are relayed when set: DHCP, TFTP, DNS, NTP (Network Time Protocol, port 123, NBNS (NetBios Name Server, port 137), NBDG (NetBIOS Datagram, port 138), and BootP.

**Specified** When set, the UDP port (1 to 65535) can be specified in the UDP Port columns (up to three per server).

**UDP Port 1, 2, 3** Used for specifying UDP ports to be relayed. These fields only apply when **UDP PORT TYPE** is set to **SPECIFIED**.

### Bridge

The **BRIDGE** menu is used to set up the bridge parameters for the 850. The bridging function runs at the Media Access Control (MAC) level which allows any protocol packets that run over Ethernet to be forwarded. Bridging can run concurrently with IP. However, when IP routing is active, IP packets (which include ARP packets) are not bridged.

### *Mode*

This is used to enable the bridge function.

### *Address Table*

The 850 automatically maintains a table of MAC addresses detected and associates those addresses with the LAN or WAN port from which they were received.

**Aging** The maximum time an idle MAC address remains in the table before being removed. The value is in minutes.

**Forward Policy** When this parameter is set to **UNKNOWN** (def), any bridge packet with a destination MAC address that is not in the bridge table is forwarded to all other ports. When set to **KNOWN**, the packet with the unknown destination MAC address is dropped and is not forwarded.

### Security

### *Authentication*

The method used for authenticating the PPP peer is selected here. The possible values are listed below.

**None** No attempt is made to authenticate the PPP peer.

**Radius** The Total Access 850 will act as a RADIUS client and authenticate the PPP peer using the RADIUS server. The Radius server parameters must be set up properly for this to work.

**PPP** The PPP profile is used to authenticate the PPP peer.

### *Radius Server*

The parameters for the RADIUS server are configured in this menu. The RADIUS server can be used for authenticating a PPP peer (if defined under **SECURITY > AUTHENTICATION**) and for Telnet server sessions.

**Primary Server** This is the IP address of the first RADIUS server that the Total Access 850 should attempt to communicate with when authenticating a PPP peer.

**Secondary Server** This is the IP address of the back-up RADIUS server that the Total Access 850 should attempt to communicate with when the primary server does not respond.

**UDP Port** This is the UDP port that the Total Access 850 should use when communicating with the RADIUS server. The default is 1645, which is the commonly used port.

**Secret** The RADIUS server and Total Access 850 share this text string. It is used by the RADIUS sever to authenticate the Total Access 850, the RADIUS client. The factory default is not to use a secret.

**Retry Count (1-10)** This is the number of times the Total Access 850 should send a request packet to the RADIUS server without a response before giving up. If the number of attempts to communicate with the primary server is equal to the retry count, the secondary server (if defined) is tried. If the secondary server does not respond within the retry count, the PPP peer (or Telnet session) is not authenticated and is dropped. The default is 5.

### *Filter Defines*

NOTE *The **FILTER DEFINES** option is for Frame Relay only.*

The Total Access 850 can filter packets based on certain parameters within the packet. The method used by the Total Access 850 allows the highest flexibility for defining filters and assigning them to a PVC. The filters are set up in two steps: (1) defining the packet types, and (2) adding them to a list under the PVC. This menu is used to define the individual filter defines based on packet type.

### *Filter Defines > MAC Filter Defines*

The MAC filter is applied to bridge packets only. Bridge packets which are forwarded by the bridge functionality of the Total Access 850 are defined here. Up to 32 MAC defines can be specified.

**Name** Identifies the filter entry.

**Src Addr** 48-bit MAC source address used for comparison. (hexadecimal format)

**Src Mask** Bits in the MAC source address which are compared. (hexadecimal format)

**Dest Addr** 48-bit MAC destination address used for comparison. (hexadecimal format)

**Dest Mask** Bits in the MAC destination address used for comparison. (hexadecimal format)

**MAC Type** 16-bit MAC type field used for comparison. (hexadecimal format)

**Type Msk** Bits in the MAC type field used for comparison. (hexadecimal format)

***Filter Defines > Pattern Filter Defines***

The pattern filter is applied to bridge packets only. That is any packet which is forwarded by the bridge functionality of the Total Access 850. Up to 32 pattern defines can be specified.

**Name** Identifies the filter entry.

**Offset** Offset from beginning of packet of where to start the pattern comparison.

**Pattern** 64 bits used for comparison. (hexadecimal format)

**Mask** Bits in the pattern to be compared. (hexadecimal format)

***Filter Defines > IP Filter Defines***

The IP filter defines apply to any IP packet, whether it is routed or bridged. Up to 32 IP defines can be specified.

**Name** Identifies the filter entry.

**IP Src** IP address compared to the source address. (dotted decimal format)

**Src Mask** Bits which are used in the source comparison. (dotted decimal format)

**IP Dest** IP address compared to the destination address. (dotted decimal format)

**Dest Mask** Bits which are used in the destination comparison. (dotted decimal format)

**Src Port** IP source port number used for comparison Range: 0 to 65535. (decimal format)

**Src Port Cmpr** Type of comparison that is performed.

**=** means ports equal to

**not =** means port not equal to

**>** means port greater than

**<** means port less than

**None -** means the source port is not compared

**Dst Port** IP destination port number used for comparison Range: 0 to 65535. (decimal format)

**Dst Port Cmpr** Type of comparison that is performed

**=** means ports equal to

**not =** means port not equal to

**>** means port greater than

**<** means port less than

**None -** means the destination port is not compared

**Proto** Protocol used for comparison. Range: 0 to 255. (decimal format)

**Proto Cmpr** Type of comparison that is performed

**=** means protocols equal to

**not =** means protocols not equal to

**>** means protocols greater than

**<** means protocols less than

**None** means the protocol is not compared

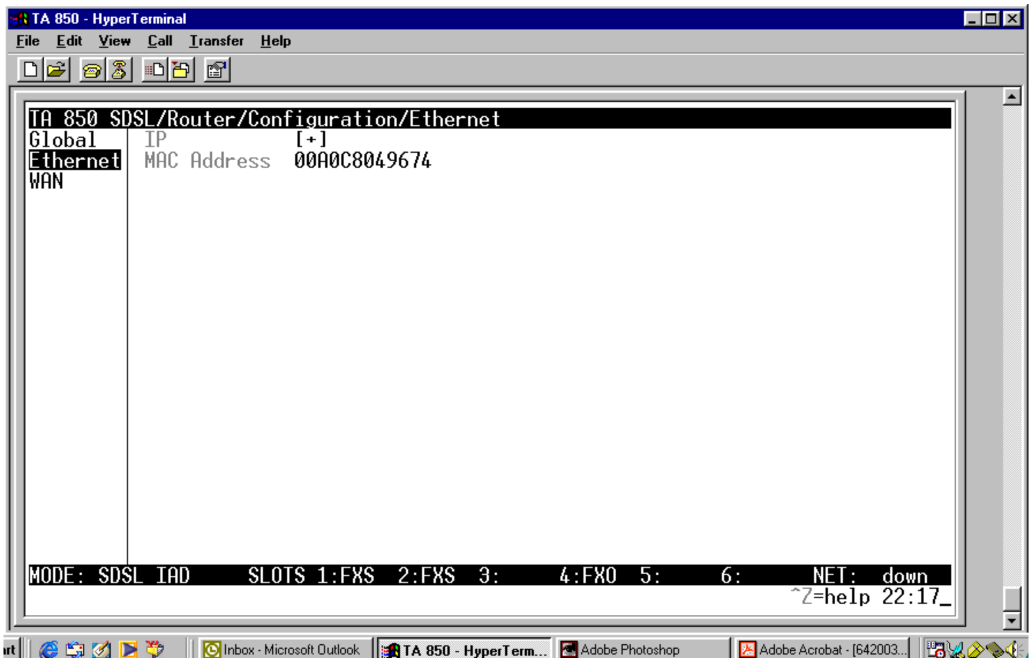
**TCP Est** **Yes -** only when TCP established

**No -** only when TCP not established

**Ignore -** ignore TCP flags

### *>Ethernet*

Use the **ETHERNET** menu (Figure 10) to configure the Ethernet port on the 850.


TA 850 - HyperTerminal
File Edit View Call Transfer Help
Inbox - Microsoft Outlook
TA 850 - HyperTerm...
Adobe Photoshop
Adobe Acrobat - [642003...]

```
TA 850 SDSL/Router/Configuration/Ethernet
Global    IP           [+]
Ethernet  MAC Address  00A0C8049674
WAN

MODE: SDSL IAD     SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET:  down
                                                                  ^Z=help 22:17_
```

**Figure 10. Ethernet Menu**

**IP**

This is used to setup the IP addresses for the LAN on the 850

***IP Address***

The IP address assigned to the 850's Ethernet port is set here. This address must be unique within the network.

***Subnet Mask***

This is the IP network mask that is to be applied to the 850's Ethernet port.

***Default Gateway***

The default gateway is used by the 850 to send IP packets whose destination address is not found in the route table.

***RIP***

Use this menu to enable RIP on the LAN interface.

**Mode** Enables or disables RIP.

**Protocol** Specifies the RIP protocol. Choices are **V1** (def) (which is RIP version 1) or **V2** (RIP version 2).

**Method** Specifies the way the RIP protocol sends out its advertisements. Choices are given below.

**None** All routes in the router table are advertised with no modification of the metrics.

**SPLIT HORIZON** Only routes not learned from this circuit are advertised.

**POISON REVERSE (def)** All routes are advertised, but the routes learned from this port are “poisoned” with an infinite metric.

**Direction** Allows the direction at which RIP advertisements are sent and listened to be specified.

**TX AND RX (def)** RIP advertisements are periodically transmitted and are listened to on this port.

**TX ONLY** RIP advertisements are periodically transmitted but are not listened to on this port.

**RX Only** RIP advertisements are not transmitted on this port, but are listened.

**V2 Secret** Enter the secret used by RIP version 2 here.

***Proxy ARP***

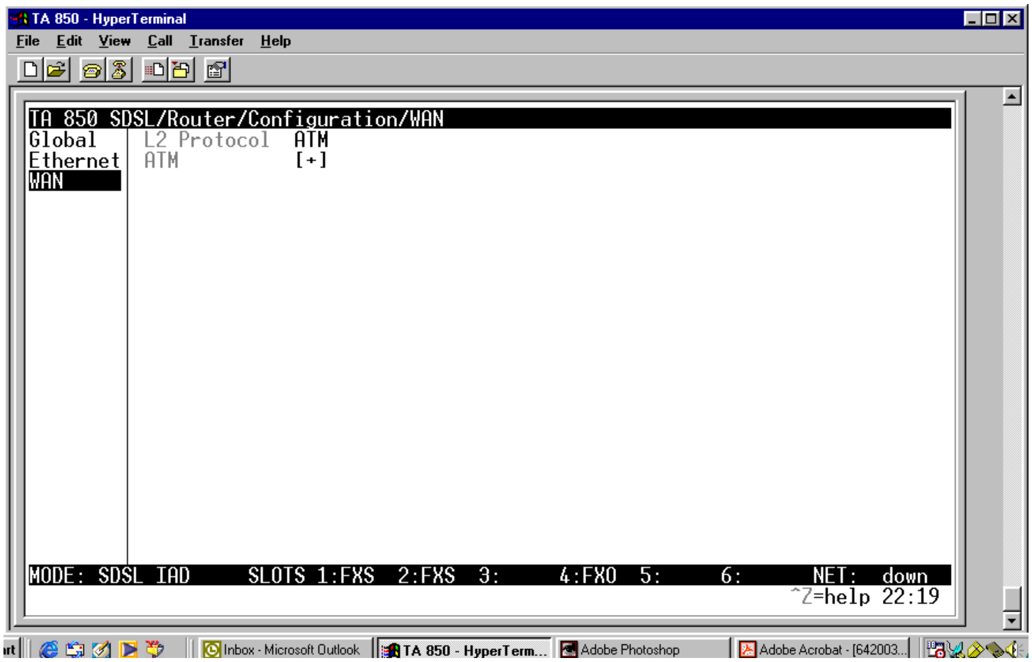
This feature allows the network portion of a group of addresses to be shared among several physical network segments. The ARP protocol provides a way for devices to create a mapping between physical addresses and logical IP addresses. Proxy ARP makes use of this mapping feature by instructing a router to answer ARP requests as a "proxy" for the IP addresses behind one of its ports. The device which sent the ARP request will then correctly assume that it can reach the requested IP address by sending packets to the physical address that was returned. This technique effectively hides the fact that a network has been (further) subnetted. If this option is set to **YES**, when an ARP request is received on the Ethernet port the address is looked up in the IP routing table. If the forwarding port is not on the Ethernet port and the route is not the default route, the 850 will answer the request with its own hardware address.

**MAC Address**

This is a read-only MAC address programmed at ADTRAN.

### *>WAN*

Use the **WAN** menu (Figure 11) to configure WAN settings on the 850.



TA 850 - HyperTerminal
File Edit View Call Transfer Help
Inbox - Microsoft Outlook
TA 850 - HyperTerm...
Adobe Photoshop
Adobe Acrobat - [642003...

```
TA 850 SDSL/Router/Configuration/WAN
Global    L2 Protocol  ATM
Ethernet  ATM          [+]
WAN







MODE: SDSL IAD      SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:       NET:  down
                                                                  ^Z=help 22:19
```

**Figure 11. WAN Menu**

**L2 Protocol**

Displays the current L2 protocol - ATM (Read Only).

**ATM**

Use the ATM menu to setup Data PVCs for the router.

***Description***

This is the text description for the PVC.

***VPI***

ATM virtual port identifier.

***VCI***

This is the ATM virtual channel identifier.

***PCR***

Peak Cell Rate for this VPI/VCI in cells/second. Cell rate that the user may never exceed.

***QOS***

Quality of Service.

***UBR***

Unspecified bit rate for data PVCs.

***Protocol***

This is the protocol supported on the PVC.

***RFC1483 IP***

Use this selection to support IP on this DLCI.

***Active***

This selection enables IP on this PVC.

***Far - End IP Address***

This is the address of the next hop router on this interface.

**IP netmask**

This is the network mask used for this interface.

***Local IP Address***

This is the IP address for this PVC.

***NAT***

Use this menu to set up and use Network Address Translation on this interface.

| | |
|---|---|
| **Network Address Port Translation** | By enabling port translation, IP packets are modified as they pass through this interface. During transmission, private addresses are translated into a single public (NAPT) IP address. Incoming packets are translated from the public to private address based on the protocol port numbers. Once enabled, you must set up NAT for use. |
| **Public IP Address Mode** | The port translation requires at least a single real IP address for translating. This value can use the IP assigned to the interface (or assigned via layer 2 protocol like PPP), obtained using DHCP client, or statically specified on this menu. If the address cannot be learned, then it must be specified in order for the translation to work. |
| **Translation Table** | Add translation entries to "fine tune" special protocols or specify private addresses. |
| **Public Address Mode** | The public IP address used for this translation entry can be the NAPT IP address assigned to the link or can be specified. You specify an address to direct packets with certain protocols to different servers. |
| **Protocol** | The upper layer protocol that is to be monitored for translation. For TCP and UDP, a port number must also be specified. |
| **Public Port Mode** | The public destination port associated with this entry can be specified to add more control over certain types of traffic. The default, **ANY PORT**, covers all port types. |
| **Private Address Mode** | The private IP address can be specified to steer certain protocols and ports to specific servers in the private network. Likewise, internal hosts can be steered to certain servers on the public network. A new request from the public network matching this entry's public parameters will be dropped if this mode is set to **ANY INTERNAL.** |

**PRIVATE PORT MODE** The private destination port associated with this entry can be specified to add more control over certain types of traffic. Leave as **ANY PORT** to cover all port types.

**TRANSLATE BODY** By default, the application payload in the packet is scanned for occurrences of the private/public IP address in binary or ASCII form. Set this to **NO** for applications where this will cause problems.

**NAT View** Shows the protocols that are actively being translated.

**NAPT Address** Represents the public address that is being used as the NAPT address.

**Entry Count** The number of entries in the NAT table.

**Entry Overflow Count** A count of the dropped entries due to low memory.

### *RIP*

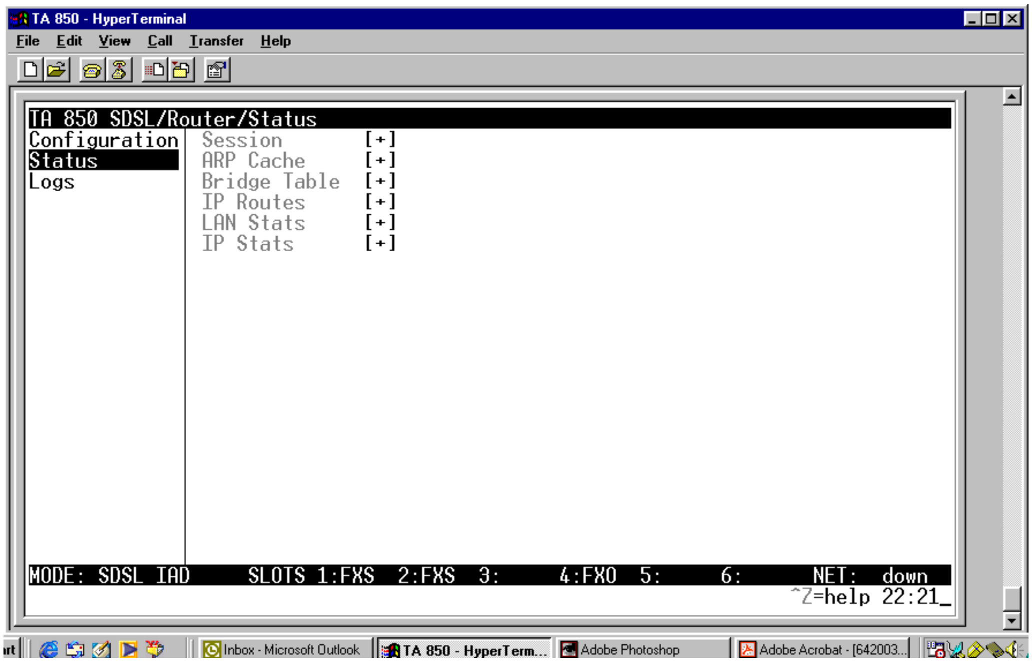
Use this menu to enable RIP on the WAN interface. (See *RIP* on page 271 for description of options.)

### RFC 1483 Bridge

This is used to enable bridge mode on this PVC.

## Configuring the Router – Status

Use the **ROUTER > STATUS** menu to view and set the parameters shown in Figure 12. The **ROUTER > STATUS** screens give the user useful information for debugging the current routes in the 850.



```
TA 850 SDSL/Router/Status
Configuration  Session      [+]
Status         ARP Cache    [+]
Logs           Bridge Table [+]
               IP Routes    [+]
               LAN Stats    [+]
               IP Stats     [+]

MODE: SDSL IAD    SLOTS 1:FXS  2:FXS  3:    4:FXO  5:    6:     NET:  down
                                                             ^Z=help 22:21_
```

Figure 12. Router > Status Menu

### *>Session*

This menu maintains statistics about the active ATM PVCs.

***>ARP cache***

This is a listing of the currently connected Ethernet port on the LAN.

***>Bridge Table***

This shows the detected MAC addresses and the interface to which they are associated.

***>IP Routes***

This shows the current routes in the 850 and their use.

***>LAN Stats***

This shows traffic over the LAN interface.

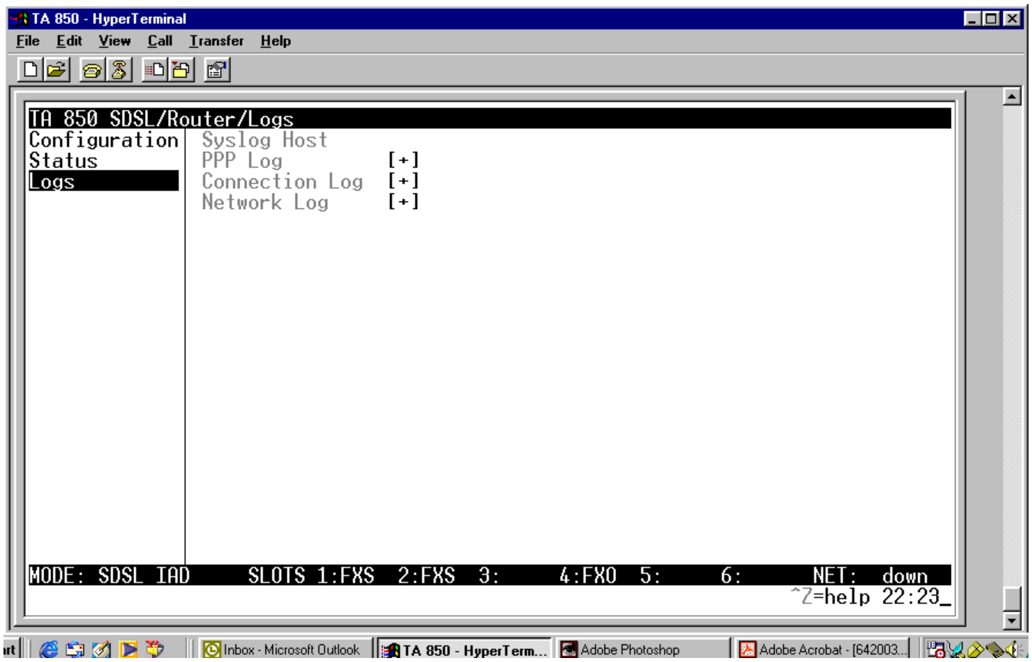
***>IP Stats***

This shows IP traffic through the 850.

## Configuring the Router – Logs

The Logs menu (Figure 13) contains logs displaying important information about the running condition of the Total Access 850. The logs can be set to capture diagnostics of error conditions only by way of a log level. The levels are divided up as follows:

level 0 - Fatal event (causes reset)
level 1 - Critical event
level 2 - Error event
level 3 - Warning event
level 4 - Notify event
level 5 - Informational event
level 6 - Debugging event


TA 850 - HyperTerminal
File Edit View Call Transfer Help
Inbox - Microsoft Outlook
TA 850 - HyperTerm...
Adobe Photoshop
Adobe Acrobat - [642003...

```
TA 850 SDSL/Router/Logs
Configuration | Syslog Host
Status        | PPP Log         [+]
Logs          | Connection Log  [+]
              | Network Log     [+]

MODE: SDSL IAD     SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET:  down
                                                                ^Z=help 22:23_
```

**Figure 13. Router > Logs Menu**

## *Sys log Host*

Set this to the IP address or domain name (if DNS configured) of the sys log host device. All log events are sent to this device.

**PPP Log**

Information pertaining to the PPP negotiation and authentication is logged in the PPP log.

**Connection Log**

Information pertaining to the call placement and answering is logged in the Connection log.

**Network Log**

Information pertaining to routing protocols is placed in this log.

Each log (PPP log, Connection log, and Network log) contains the following elements.

***Active***

When set to **YES** (def), PPP events below or equal the log level are logged into the log.

***Wrap***

When set to **YES** (def), new PPP events will overwrite old PPP events when the log is full. All logging will stop when the log is full and set to **NO**.

***Level***

In order to log events, they must be at or below this level. Range is 0 to 6. The default is 3.

***View***

This menu displays the log list. The fields are as follows:

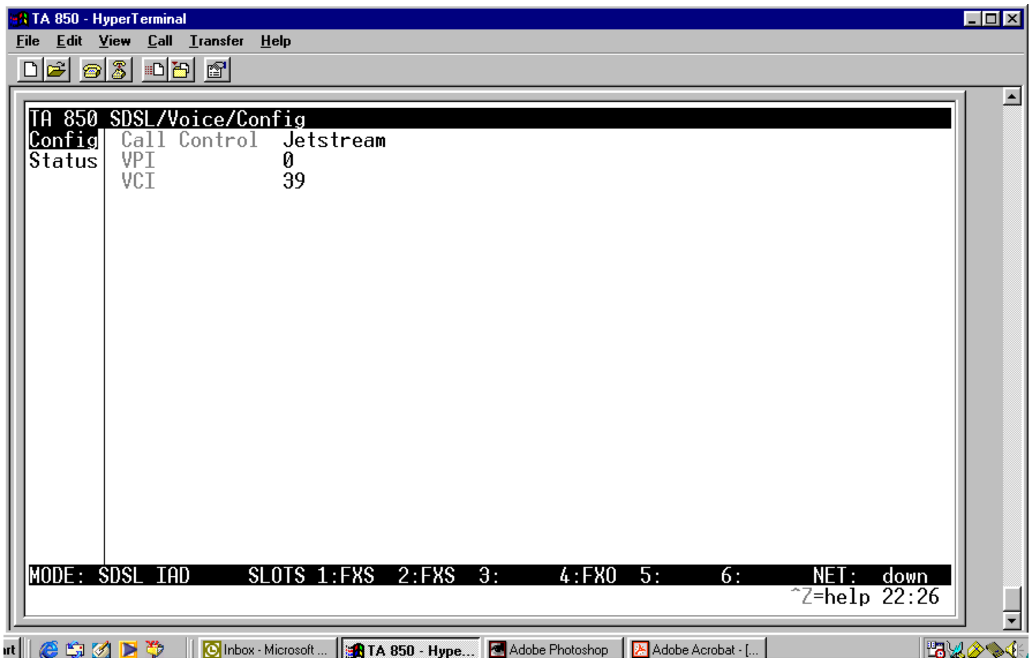
| | |
|---|---|
| **Date/Time** | Date and time event occurred. The log does not display actual time. |
| **Level** | Level associated with this event (0-6). |
| **Message** | Text message for this event. If message is too long to fit on the line, another event appears below it continuing the message. |

***Clear***

This clears the log when activated.

## Configuring Voice Support – Config

Use the **VOICE > CONFIG** menu to view and set the parameters shown in Figure 14.



```
TA 850 SDSL/Voice/Config
Config  Call Control   Jetstream
Status  VPI            0
        VCI            39

MODE: SDSL IAD     SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET:  down
                                                                ^Z=help 22:26
```

**Figure 14. Voice > Config Menu**

### *>Call Control*

The **CALL CONTROL** setting is used to configure the correct Voice Gateway protocol for voice signaling control between the Total Access 850 and the configured Gateway. The **CALL CONTROL** setting must be configured correctly before the voice circuits will work correctly. The Total Access 850 supports Jetstream, Tollbridge, and CopperCom Voice Gateways.

### *>VPI*

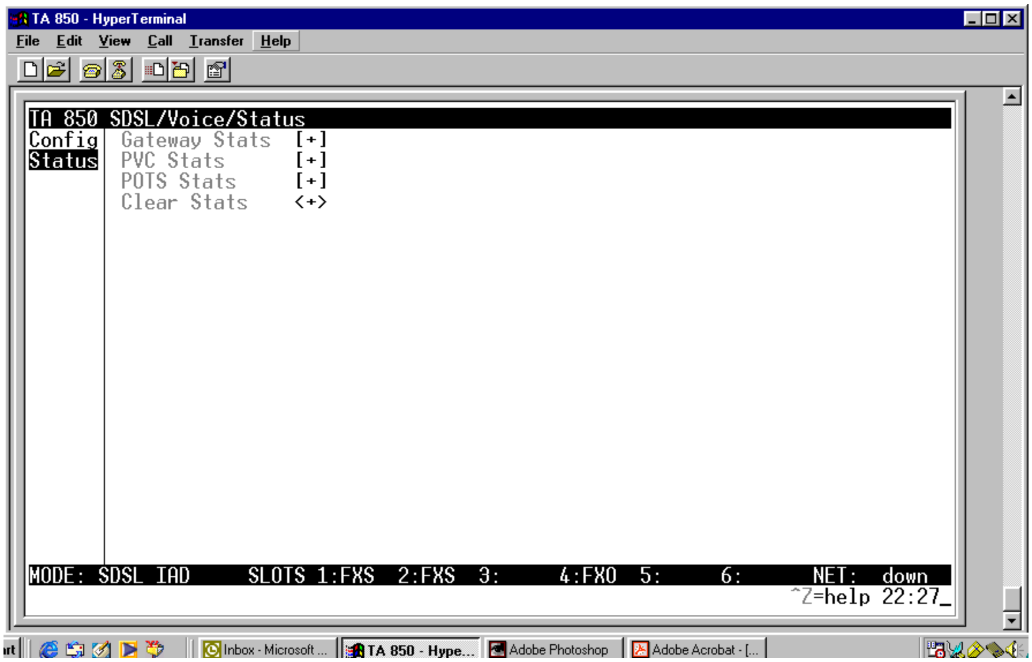
The **VPI** setting is used to configure the Total Access 850 virtual path setting used to communicate with the configured Voice Gateway.

### *>VCI*

The **VCI** setting is used to configure the Total Access 850 virtual circuit setting used to communicate with the configured Voice Gateway.

## Configuring Voice Support – Status

Use the **VOICE > STATUS** menu to view and set the parameters shown in Figure 15.



```
TA 850 SDSL/Voice/Status
Config  Gateway Stats   [+]
Status  PVC Stats       [+]
        POTS Stats      [+]
        Clear Stats     <+>

MODE: SDSL IAD     SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET:  down
                                                          ^Z=help 22:27_
```

**Figure 15. Voice > Status Menu**

### *>Gateway Stats*

The **GATEWAY STATS** menu shows the current state of the communication link between the Total Access 850 and the Voice Gateway. The Gateway Link is indicated as **UP** or **DOWN**. A count of management messages is indicated along with the number of active calls in progress.

### *>PVC Stats*

The **PVC STATS** menu shows the current state of the virtual circuit used between the Voice Gateway and the Total Access 850 IAD for voice signaling and voice payload delivery.

### *>POTS Stats*

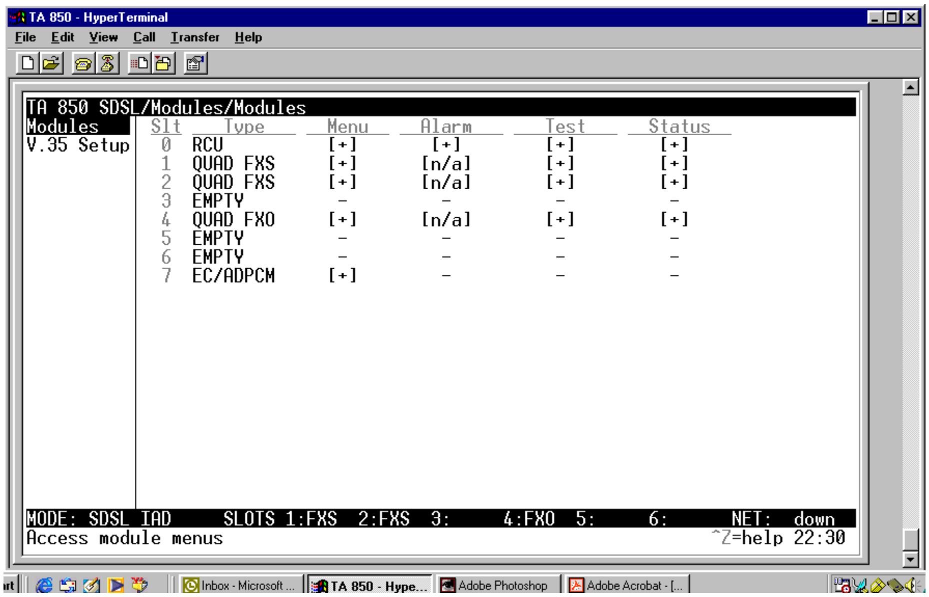
The **POTS STATS** menu shows real-time indication status of each voice port on the Total Access 850. From this menu, on a per port basis, the user can determine which ports are active/inactive. Several statistics at this menu are used only for internal ADTRAN development. Task, Inserts, and Drops indicators are for internal use only.

### *>Clear Stats*

The **CLEAR STATS** menu can be used to clear the counters used for Voice Status menus.

## Managing the Modules – Modules

Use the **MODULES** menu to view and set the parameters shown in Figure 16.



```
TA 850 SDSL/Modules/Modules
Modules    Slt   Type       Menu     Alarm      Test      Status
V.35 Setup  0   RCU         [+]       [+]        [+]       [+]
            1   QUAD FXS    [+]      [n/a]       [+]       [+]
            2   QUAD FXS    [+]      [n/a]       [+]       [+]
            3   EMPTY        -         -          -         -
            4   QUAD FXO    [+]      [n/a]       [+]       [+]
            5   EMPTY        -         -          -         -
            6   EMPTY        -         -          -         -
            7   EC/ADPCM    [+]        -          -         -

MODE: SDSL IAD      SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET: down
Access module menus                                              ^Z=help 22:30
```

**Figure 16. Modules Menu**

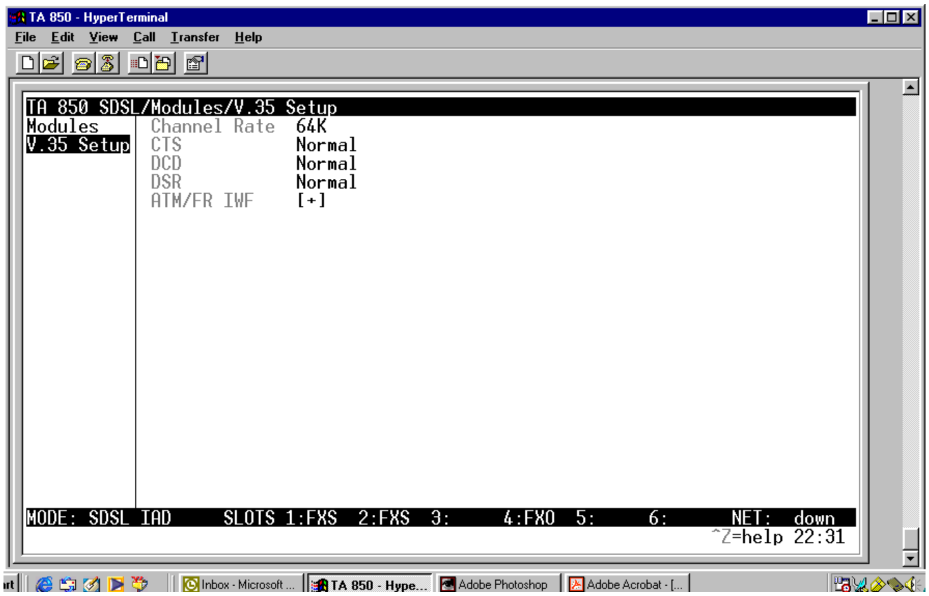
### >Modules Table

The **MODULES** table indicates the type and slot number of each module installed in the Total Access 850 and is used to manage these modules.

The table contains **MENU**, **ALARM**, **TEST**, and **STATUS** indicators/menus customized for each module.

## Managing the Modules – V.35 Setup

Use the **V.35 SETUP** menu to view and set the parameters shown in Figure 17.



```
TA 850 SDSL/Modules/V.35 Setup
Modules    Channel Rate   64K
V.35 Setup CTS            Normal
           DCD            Normal
           DSR            Normal
           ATM/FR IWF     [+]

MODE: SDSL IAD      SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET: down
                                                                 ^Z=help 22:31
```

**Figure 17. V.35 Setup Menu**

**Channel Rate** and **EIA** settings are supported via this menu option. For all typical applications, these settings are left in their default states.

## *>ATM/FR IWF*

This menu contains the setup and status for the ATM/Frame Relay interworking functions.

### Mode

The **Mode** setting configures the V.35 port for FRF5 or FRF8 operation, depending upon the application being supported.

#### *FRF5*

This is also known as Network Interworking. Use this mode for Frame Relay over ATM.

#### *FRF8*

This is also known as Service Interworking. In this mode, the Total Access 850 performs a translation between Frame Relay and ATM protocols.

### Configuration

The **Configuration** menu is used to support the configuration of Frame-to-ATM interworking, signaling formats, timeout values, and PVC settings.

The following settings are used for FRF5.

| | |
|---|---|
| **Lan FR Maint Protocol** | Frame Relay maintenance or signaling protocol between local V.35 port and the attached DTE port, support ANSI Annex A, CCITT Q933 Annex D, CISCO LMI or Static (no signaling). |
| **Lan FR Poll Timeout T392 (5-30)** | T392 for signaling protocol, typical value 15. No meaning if Maint Protocol is Static. |
| **FRN Port Config** | Logical Frame Relay ports over ATM. Up to 4 ports are supported with each port supporting up to 4 DLCI mappings. Go to **Num** field. Typing "i" or "I" will insert another entry, and typing "d" or "D" will delete one entry. |
| **Name** | To identify your port. |
| **ATM VPI** | Specifies the virtual path over which this logical port is running. |
| **ATM VCI** | Specifies the virtual circuit over which this logical port is running. |
| **PCR** | Peak Cell Rate for this VPI/VCI in<br>cells/second. Cell rate that the user may never exceed. |
| **QOS** | Quality of Service.<br>UBR - unspecified bit rate for data PVCs. |
| **De Map** | Frame Relay to ATM demapping; default value (Frn Only, ATM 0) suggested. |
| **CLPI Map** | ATM to Frame Relay CLPI map; default value (Frn Only) suggested. |
| **D/C** | Set D/C field in the header to 0 or 1. |
| **Header** | Header format; only 2 bytes supported now. |

**Maint Protocol** Maintenance or signaling protocol over this logical Frame Relay port. Support Annex A, Annex D, CISCO LMI or Static.

**Mux Mode** Many DLCIs or one DLCI mapping over this port.

**DLCI Map** Actual DLCI mappings.

**Active** Always active, not configurable.

**Lan DLCI** The DLCI configured over local V.35 Frame Relay port.

**Net DLCI** The DLCI configured over the WAN side logical Frame Relay port.

The following settings are used for FRF8.

**Lan FR Maint Protocol** Frame Relay maintenance or signaling protocol between local V.35 port and the attached DTE port, support ANSI Annex A, CCITT Q933 Annex D, CISCO LMI or Static (no signaling).

**Lan FR Poll Timeout T392 (5-30)** T392 for signaling protocol, typical value 15. No meaning if Maint Protocol is Static.

**Fr/ATM PVC Mapping** Up to 4 mappings are supported.

**FR DLCI** Frame Relay DLCI on V.35 port.

**ATM VPI** Specifies the virtual path to which DLCI is mapped.

**ATM VCI** Specifies the virtual circuit to which DLCI is mapped.

**PCR** Peak Cell Rate for this VPI/VCI in cells/second. Cell rate that the user may never exceed.

**QOS** Quality of Service.
UBR - unspecified bit rate for data PVCs.

**Translate** Translate or transparent mode between Frame Relay frames and ATM cells.

**De Map** Map Frame Relay DE bit to ATM CLPI bit, Always 0, Always 1 or Convert each other.

**Fecn Map** Map Frame Relay FECN bit to ATM EFCI bit, Always 0, Always 1 or Convert each other.

## Appendix A. Voice Gateway Quick Start Procedure (Voice Turn up)

A typical VoDSL application (see Figure 18) uses a Total Access 850 connected to an ATM network. For voice applications, a Voice Gateway is needed to interface with the PSTN. Jetstream, Tollbridge, and CopperCom are popular Gateway types.

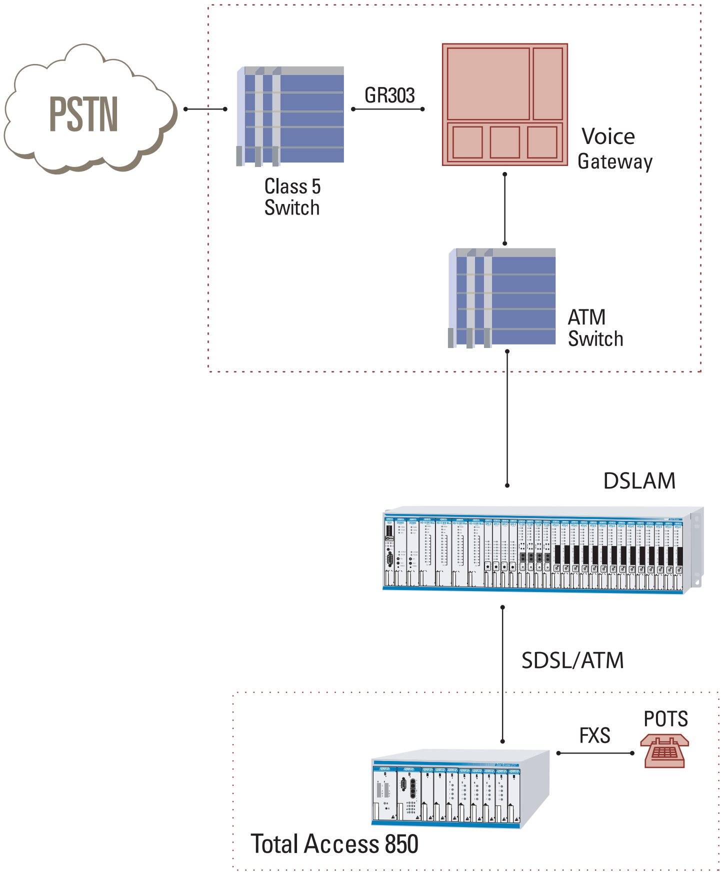


**Figure 18. Application Diagram**

To configure a Total Access 850 for use with the Voice Gateway, you need to know the VPI and VCI to be used on the ATM network. You also need to know the format for Idle Cells and whether Data Scrambling is used on this ATM network. The following procedure will help you navigate the Total Access 850 menus for configuring the necessary elements for VoDSL with a Voice Gateway.

| Voice Turn Up | |
|---|---|
| **Step** | **Action** |
| **1** | From the Total Access 850 main menu, select the **WAN** menu. (Here you set up the ATM network.) |
| **2** | Select the **ATM CONFIG** menu. |
| **3** | Enter the **IDLE CELLS** format for your network. |
| **4** | Set **DATA SCRAMBLING** appropriately for your network. |
| **5** | Back all the way out to the top level Total Access 850 menu, and then select the **VOICE** menu. (From this menu, the appropriate Voice information for working with the Voice Gateway is entered.) |
| **6** | Select **CONFIG**, and from the **CONFIG** menu, enter the Gateway type under **CALL CONTROL** and enter the VPI and VCI values for communicating with that Gateway.<br>For this application, **CALL CONTROL** should be set to the Gateway type and the VPI and VCI values should be set appropriately for your network. |
| **7** | To verify correct setup, use the **STATUS** menu (under the **VOICE** menu) to look at the current status of the voice connection.<br>Under **STATUS**, you can view the **GATEWAY STATS** and information about the voice PVC along with information about the POTs ports available on the Gateway.<br>The **GATEWAY STATS** menu should show the Gateway Link is up (if everything is configured correctly). |

## Appendix B. RFC1483 Quick Start (IP Routing)

The Total Access 850 allows for complete integration of voice and data delivery from one compact platform (see Figure 19). Once you have completed the voice turn up procedure from the previous example, adding data to the circuit requires some additional setup.

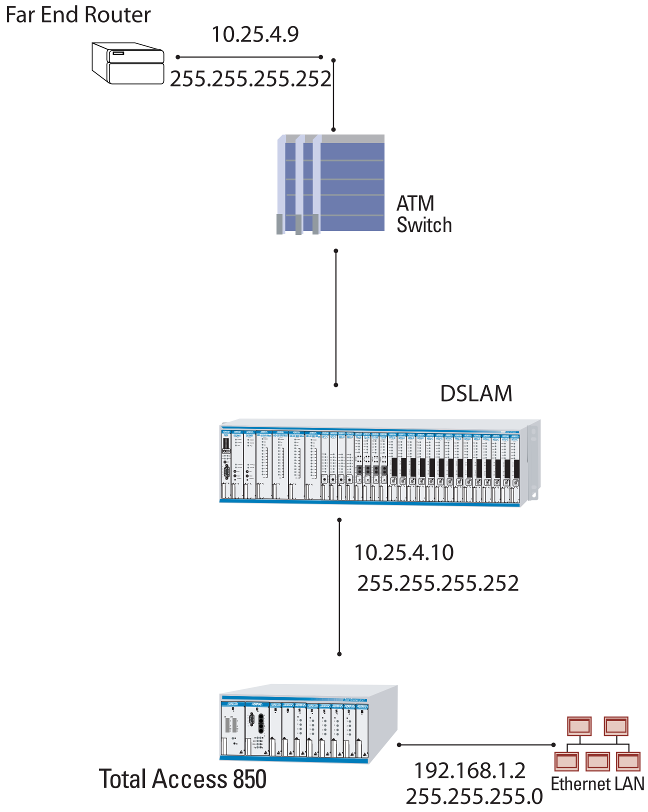


**Figure 19. Application Diagram**

To configure a Total Access 850 for IP routing, you need to know the VPI and VCI values for the data circuit on your network. You also need the IP address of the next hop router in the circuit.

The table on the next page shows how to configure the Total Access 850 for IP Routing.

.

| IP Routing | |
|---|---|
| **Step** | **Action** |
| **1** | From the Total Access 850 main menu, select the **WAN** menu. (Here you set up the ATM network.) |
| **2** | Select the **ATM CONFIG** menu. |
| **3** | Enter the **IDLE CELLS** format for your network. |
| **4** | Set **DATA SCRAMBLING** appropriately for your network. |
| **5** | Back all the way out to the top level Total Access 850 menu, and then select the **ROUTER** menu. |
| **6** | Select **CONFIGURATION**.<br>From the **CONFIGURATION** menu, you will set up addresses for your LAN and WAN.<br>For basic IP routing, use all the default values from the **GLOBAL** menu. |
| **7** | From the **ETHERNET** menu, enter the **IP** menu to enter your LAN configuration. |
| **8** | Enter your LAN **IP ADDRESS**, **SUBNET MASK**, and **DEFAULT GATEWAY** information.<br>For this example, the **IP ADDRESS** is 192.168.1.2, the **SUBNET MASK** is 255.255.255.0, and the **DEFAULT GATEWAY** is 10.25.4.9. |
| **9** | Arrow back to the main **ROUTER CONFIGURATION** menu, and select the **WAN** menu and then the **ATM** menu. (Here you will enter your data PVC information.) |
| **10** | Create a new PVC by entering the menu. Enter your VPI and VCI values. |
| **11** | From the **RFC1483 IP** menu, enter your WAN information.<br>For this example, the **FAR END IP ADDRESS** is 10.25.4.9, the **IP NETMASK** is 255.255.255.252, and the **LOCAL IP ADDRESS** is 10.25.4.10. |
| **12** | Arrow back to the top level Total Access 850 menu to activate your changes. |

## Appendix C. RFC1483 Quick Start (IP Routing with NAT)

To illustrate the use of NAT, consider the example from Appendix B. To set up a single public address that will be used to access the public network, you will use the **NAT** menu on the **WAN > ATM > RFC1483 IP** menu.

| IP Routing with NAT | |
|---|---|
| **Step** | **Action** |
| **1** | The NAT menu is found under **TA 850 > SDSL > ROUTER > CONFIGURATION > WAN > ATM > RFC 1483 IP > NAT**. |
| **2** | From the **NAT** menu, set **NETWORK ADDRESS TRANSLATION** to **ENABLED**. (This will enable translation and populate the corresponding NAT menu options.) |
| **3** | Set **PUBLIC IP ADDRESS MODE** to either **INTERFACE** or **SPECIFIED**.<br>• **INTERFACE** is the default and will use the WAN IP address for the NAPT address.<br>• **SPECIFIED** allows you to enter another public address for private addresses to be translated into.<br>For basic NAT, this is all of the configuration that needs to be done.<br>For specific port translations or 1:1 mapping, you can enter **TRANSLATION TABLE** [+]. |

| IP Routing with NAT (Continued) | | |
|---|---|---|
| **4** | From the **Translation Table** menu, create a new entry by using the right arrow to enter the table. | |
| **5** | Create specific NAT translations based on your application. | |
| | **Public Address Mode** | **NAPT Addr** (Address) or **Specified**. Choice of using the NAPT address or specifying a different public address to be used for this translation. |
| | **Protocol** | Protocol for this translation. (TCP, UCP, ICMP) |
| | **Public Port Mode** | **Specified** or **Any Port**. Choosing **Specified** brings up the **Public Port** and **Public Port Type** (read-only) settings. |
| | **Public Port** | Numeric Public Port number to be translated (i.e., 23, 80). |
| | **Public Port Type** | Read-only port type chosen by the user setting of the **Public Port** option. |
| | **Private Address Mode** | **Specified** or **Any Internal**. Choosing **Specified** brings up the **Private Address** option. |
| | **Private Port Mode** | **Specified** or **Any Port**. Choosing **Specified** brings up the **Private Port** option. |
| | **Private Port** | Numeric Private Port number to be translated to (i.e. 23, 80). |
| | **Translate Body** | **Yes** or **No**. If set to **Yes**, this will translate the body of the data packet and replace the private address with the NAPT address. Default is **No**, which is used for most applications. |

## Appendix D. RFC1483 Quick Start (Bridging)

The Total Access 850 allows for complete integration of voice and data delivery from one compact platform. Once you have completed the voice turn up procedure from the previous example, adding data to the circuit requires some additional setup.

To configure a Total Access 850 for Bridging, you need to know the VPI and VCI values for the data circuit on your network.

| Bridging | |
|---|---|
| **Step** | **Action** |
| **1** | From the Total Access 850 main menu, select the **WAN** menu. (Here you set up the ATM network.) |
| **2** | Select the **ATM CONFIG** menu. |
| **3** | Enter the **IDLE CELLS** format for your network. |
| **4** | Set **DATA SCRAMBLING** appropriately for your network. |
| **5** | Back all the way out to the top level Total Access 850 menu, and then select the **ROUTER** menu. |
| **6** | Enter the **CONFIGURATION** menu.<br>From this menu, you will set up addresses for your LAN and WAN.<br>For bridging, you need to turn off **GLOBAL IP ROUTING** and turn on **GLOBAL BRIDGING**. |
| **7** | From the **ETHERNET** menu, enter the **IP** menu to enter your LAN configuration. |
| **8** | Enter your LAN **IP ADDRESS** and **SUBNET MASK**.<br>For this example, the **IP ADDRESS** is 192.168.1.2 and the **SUBNET MASK** is 255.255.255.0. |
| **9** | Arrow back to the main **ROUTER CONFIGURATION** menu, and select the **WAN** menu and then the **ATM** menu. (Here you will enter your data PVC information.) |
| **10** | Create a new PVC by entering the menu. Enter your VPI and VCI values. |
| **11** | Disable IP on the **RFC1483 IP** menu and enable Bridging on the **RFC1483 BRIDGE** menu. (This enables the Total Access 850 as a bridge.) |
| **12** | Arrow back to the top level Total Access 850 menu to activate your changes.<br>All packets that come in on the Ethernet will be forwarded on the WAN. |

## Appendix E. Routing in HDIA Mode

The Total Access 850 allows for complete integration of voice and data delivery from one compact platform. The CopperMountain DSLAM uses Frame Relay instead of ATM as their Layer 2 protocol. Once you have completed the Layer 1 configuration from the previous examples, you must configure the Layer 2 protocol. Refer to Figure 20 on page 290 as you complete the steps below.

**Frame Relay Setup**

| Step | Action |
|---|---|
| 1 | From the **IAD > Wan > Frame Relay Config** menu, select **Maintenance Protocol.** Set **Maintenance Protocol** to **Static.** |
| 2 | From the **IAD > Wan > Frame Relay Config** menu, select **DLCI Mapping**. |
| 3 | On the **DLCI Mapping** menu, **DLCI 528** should be selected. Right arrow to the **IP Map** menu. |
| 4 | On the **IP Map** menu, set up the following:<br>Set **Active** to **Yes w/Bridge Encapsulation.**<br>Set **IARP** to **Yes.**<br>Set **Far-end IP Address** to the next hop router on the ATM interface connected to the Copper Mountain for this DSL line (10.100.2.145 in Figure 20).<br>Set IP Netmask appropriately for this interface.<br>Set **Local IP Address** to the Copper Mountain IP address for this line (10.100.2.148 in Figure 20). |
| 5 | On the **Nat** menu, set up the following:<br>Set **Network Address Port Translation** to **Enabled.**<br>Set **Public IP Address Mode** to **Specified.**<br>Set **Public IP Address** the same as **Local IP Address** above.<br>From the **Translation Table**, set up the following (create entries so that the appropriate protocols are translated):<br>Right arrow to create an entry.<br>Keep the defaults to enable TCP translation.<br>Press **I** over the 1 in the first entry to create entry 2.<br>Change the Protocol to ICMP for this entry.<br>Continue creating entries as appropriate for each application. |
| 6 | Arrow back (left arrow) to the **IAD > Wan > Frame Relay Config > DLCI Mapping** menu. |
| 7 | From the **Bridge Map** menu, set **Active** to **No.** |

| Frame Relay Setup (Continued) | |
|---|---|
| **8** | Arrow back to the **IAD > ROUTER** menu. Select **CONFIGURATION.** |
| **9** | On the **GLOBAL** menu, set up the following:<br>Select **IP**.<br>Set **MODE** to **ON**.<br>Select **DHCP SERVER**.<br>Set **DHCP MODE** to **ON**.<br>From **DOMAIN NAMES**, set up the following:<br>Set **PRIMARY DNS** appropriately (172.22.48.47 in Figure 20).<br>Set **SECONDARY DNS** appropriately (172.22.48.1 in Figure 20).<br>Select **BRIDGE**.<br>Set **MODE** to **OFF**. |
| **10** | Arrow back to the **ETHERNET** menu, and set up the following:<br>Select **IP**.<br>Set **IP ADDRESS** appropriately for your LAN (10.0.0.1 in Figure 20).<br>Set **SUBNET MASK** appropriately**.**<br>Set **DEFAULT GATEWAY** to the ATM router connected to the Copper Mountain (10.100.2.145 in Figure 20). |

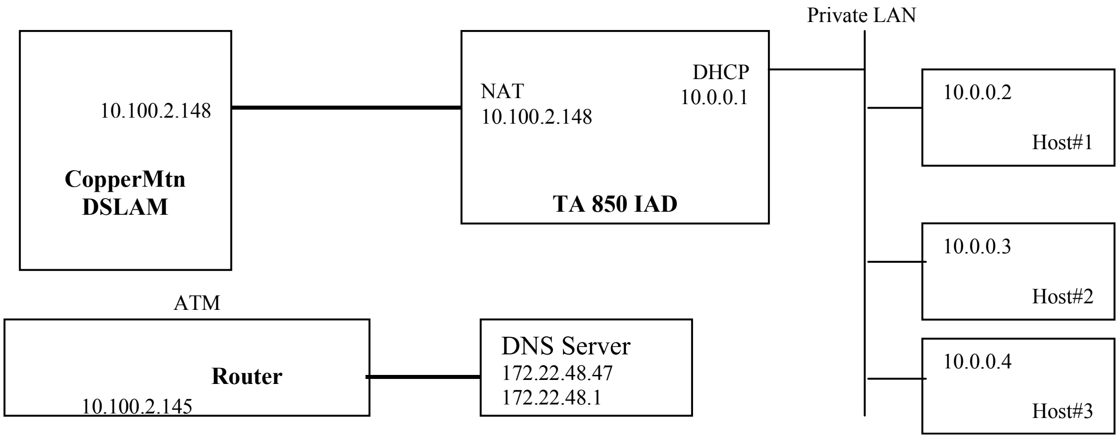


**Figure 20. Routing with Copper Mountain**

# DETAIL LEVEL PROCEDURES

# CONNECTING THE ALARM CONTACTS AND THE EXTERNAL INPUT

### *Introduction*

This DLP explains how to connect the alarm contacts and the external input on the Total Access 850.

### *Prerequisite Procedures*

Before making alarm connections, the unit should be mounted in its permanent location.

### *Tools and Materials Required*

- Small Phillips screwdriver

| | |
|---|---|
| WARNING | *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.* |

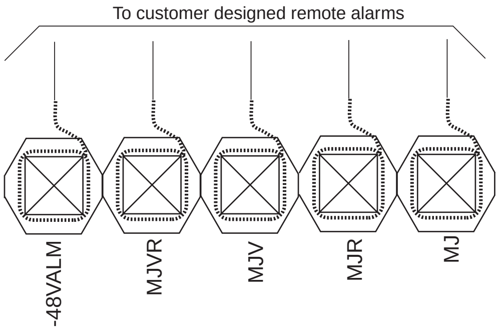
| | |
|---|---|
| CAUTION | *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.* |

# DLP-001

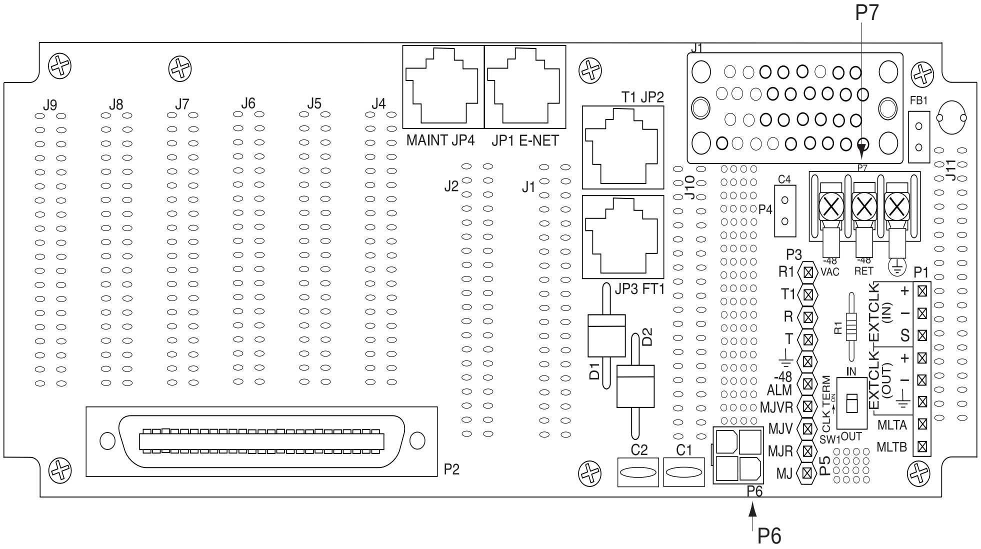
## Perform Steps Below in the Order Listed

1. Backplane alarm connections (P5) are labeled as shown in the table below and illustrated in the figure.

| **P3 Wire-Wrap Connections** | | |
|---|---|---|
| T1 Connections | | |
| 1 | R1 | DS1 Ring input from network |
| 2 | T1 | DS1 Tip input from network |
| 3 | R | DS1 Ring output from network |
| 4 | T | DS1 Tip output from network |
| 5 | Gnd | Ground |
| **P5 Wire-Wrap Connections** | | |
| Alarm Connections | | |
| 1 | -48 ALM | DC Alarm output |
| 2 | MJVR | Major Alarm Visual Common |
| 3 | MJV | Major Alarm Visual |
| 4 | MJR | Major Alarm Audible Common |
| 5 | MJ | Major Alarm Audible |



NOTE *You will have to remove the cover to access the contacts. Refer to the Total Access 850 rear view illustration on the next page.*



2. **Alarm relay contacts are open during normal operation. The alarm relay contacts close in the event of a local alarm condition or the receipt of an alarm from the T1 Carrier.**

3. **In a carrier alarm condition such as a Red, Yellow, or Blue (unframed all 1s), various alarm contacts in the PSU close.**

4. **Carrier alarm conditions cause the Total Access 850 to initiate trunk processing. The following chain of events then occur:**

   - MJ will be directly shorted to MJR.
   - MJV will be directly shorted to MJVR.

5. **Contacts MJ and MJR can be overridden manually during an alarm condition by pressing the ACO pushbutton on the PSU faceplate.**

6. **If the 3-Amp power fuse on the PSU trips, the -48 ALM relay will close, providing a -48 VDC signal on that pin. This alarm cannot be overridden by the ACO pushbutton. Refer to the table below for alarm notifications.**

| **Alarm Condition** | **Relays Activated** | | |
|---|---|---|---|
| | **MJR** | **MJVR** | **-48 ALM** |
| Red Alarm | X | X | |
| Yellow Alarm | X | X | |
| AIS Alarm | X | X | |
| PSU Power Fuse Fails | X | X | X |
| Alarms ACO Deactivates | X | X | |
| **Note: ACO will not deactivate MJR after a power fuse failure.** | | | |

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# SETTING IP PARAMETERS FOR THE TOTAL ACCESS 850

### *Introduction*

If the Total Access 850 is connected to an IP network for Telnet, TFTP, or SNMP management, there are several IP parameters that must be set in order for the unit to communicate with the network. These parameters are described in this DLP along with the procedures for setting them.

> NOTE *Please see your Network Administrator for the proper assignment of the following parameters: IP Address, Subnet Mask, and Default Gateway.*

### *Prerequisite Procedures*

This procedure assumes that the Total Access 850 unit is connected to an IP network and is powered up.

### *Tools and Materials Required*

- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access 850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU **CRAFT** port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary.
- Ethernet cable from 10BaseT port on Total Access 850 to hub (customer-provided)
- Use Ethernet crossover if going from Total Access 850 to PC

> WARNING *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

> CAUTION *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.*

# DLP-002

**Perform Steps Below in the Order Listed**

1. **Connect the Total Access 850 unit to your VT-100 system (details found in *DLP-005, Connecting the Terminal or PC to the CRAFT Port*).**

2. **Log in to the system with maximum rights (details for logging in are in ).**

3. **From the ROUTER CONFIG menu, select the INTERFACES option and press <Enter>.**

4. **From the ROUTER CONFIG/INTERFACES menu, select SETUP, then the PRIMARY IP option and press <Enter>. Select IP ADDRESS and press <Enter>.**

   Enter the appropriate IP address.

5. **From the ROUTER CONFIG/INTERFACES/PRIMARY IP menu, select the SUBNET MASK option and press <Enter>.**

   Enter the appropriate Subnet Mask.

6. **From the ROUTER/CONFIG/ROUTES IP menu, select the DEFAULT GATEWAY option and press <Enter>.**

   Enter the appropriate Default Gateway.

7. **Escape out to the ROUTER CONFIG menu and logoff by pressing <Ctrl + L>.**

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# VERIFYING COMMUNICATIONS OVER AN IP LAN

### *Introduction*

When an Ethernet Port is connected to a local area network (LAN), test steps must be performed on the Total Access 850 to ensure that the unit is communicating properly over the network. This procedure outlines those steps.

### *Prerequisite Procedures*

Before beginning this procedure, the unit should be physically connected to the LAN and the provisioning tasks detailed in  should be complete.

### *Tools and Materials Required*

- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access 850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU **CRAFT** port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary.
- Ethernet cable from 10BaseT port on Total Access 850 to hub (customer-provided)
- Use Ethernet crossover if going from Total Access 850 to PC.

| | |
|---|---|
| **WARNING** | *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.* |

| | |
|---|---|
| **CAUTION** | *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.* |

# DLP-003

**Perform Steps Below in the Order Listed**

1. Ascertain the Total Access 850 IP address.

   If you do not already have the IP Address for the Total Access 850, either obtain it from the Network Administrator or manually check for the address in the **ROUTER CONFIG > INTERFACE > SETUP > PRIMARY IP > IP ADDRESS** menu of the Network Management interface.

> NOTE *You must login with a security level of 2 to modify the IP parameters on the Total Access 850.*

**2. Ping the Total Access 850 unit from a remote computer on the network.**

Using a remote computer system connected to the LAN, perform an ICMP Ping on the IP Address of the Total Access 850. Verify that the unit responds properly.

If the Total Access 850 fails to respond, try the following:

- Verify that the proper IP Address, Subnet Mask, and Default Gateway are provisioned in the unit (see for details).
- Verify that the Total Access 850 is properly cabled into the LAN and that the ethernet cable is properly seated in the RJ-45 LAN port on the rear of the unit.
- Verify the link light on the RCU is lit. If not lit, check the cabling between the hub and the shelf.
- If the Total Access 850 is connected to a hub or other network device that provides a carrier sense light for each port, verify that the carrier sense light for the port to which the Total Access 850 is connected is lit. If this light is not lit, check the cabling between the hub and the shelf.
- Verify the IP Address, Subnet Mask, and Default Gateway on the remote computer system.
- Use Ethernet straight-through cable for connection to hub or switch. Use Ethernet crossover if connecting to PC.

If none of these steps are successful, contact the LAN Administrator for assistance.

> NOTE *Refer to the documentation of the computer system if you are unsure how to perform a Ping command. Most computers running a networked version of Microsoft Windows™ or UNIX allow a Ping to be performed by simply typing "ping <IP Address>" at a command line prompt. Typically, the Ping program will respond by indicating that the remote IP Address has responded in a certain amount of time or that no response was received.*

> NOTE *Some versions of Ping will continue running until you explicitly tell them to stop. If the program does not terminate on its own, type* **<Ctrl+C>** *to get the program to stop.*

**3. Telnet to the Total Access 850.**

From the same computer used in the previous step, Telnet to the Total Access 850 and verify that the Telnet session is properly opened (see DLP-011, *Connecting to the ATLAS 850 Using Telnet*). Once the Telnet session is established, press **<Ctrl+L>** to logout and close the session.

> NOTE *Refer to the documentation of the computer system if you are unsure how to perform a Telnet. Most computers running a networked version of Microsoft Windows™ or UNIX allow a Telnet to be performed by simply typing "Telnet <IP Address>" at a command line prompt. Telnet is a utility common on many local area networks that allows remote access to another computer or piece of equipment.*

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# LOGGING IN TO THE SYSTEM

### *Introduction*

Once connected to the Total Access  850 via either a VT-100 terminal or PC configured as a VT-100 terminal, it is necessary to login to the system to gain access to the management and provisioning functions. This DLP provides specific steps for logging in to the system and accessing the various management and provisioning functions.

### *Prerequisite Procedures*

Complete DLP-005, *Connecting the Terminal or PC to the CRAFT Port*, before logging in to Total Access 850.

### *Tools and Materials Required*

- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access  850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU **CRAFT** port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary.

**WARNING**

*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

**CAUTION**

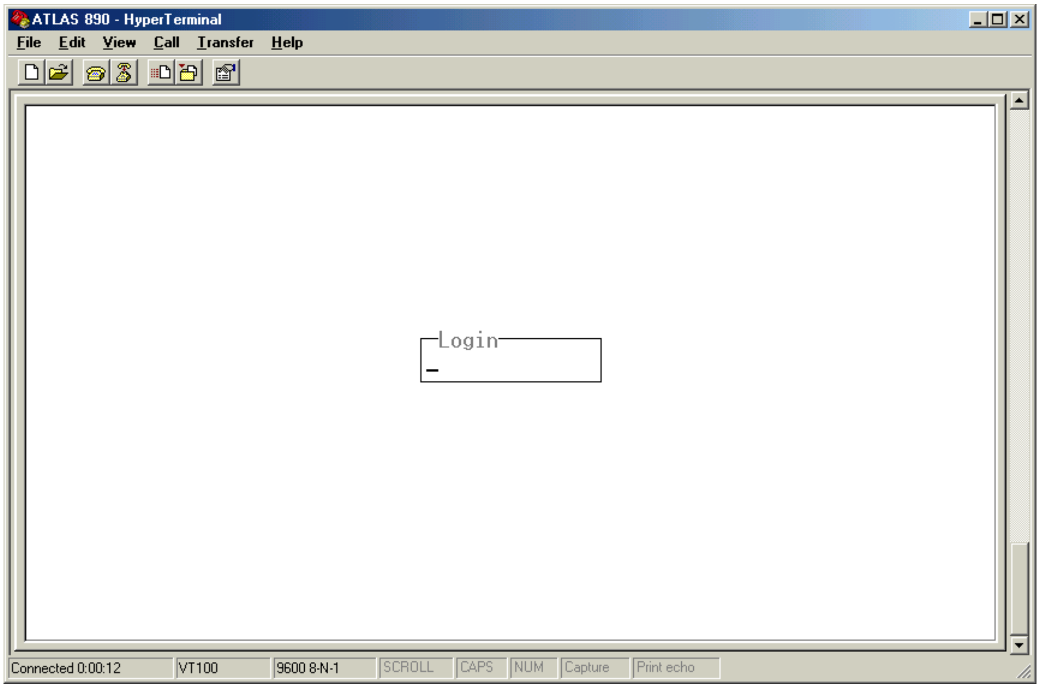
*Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.*

# DLP-004

## Perform Steps Below in the Order Listed

1. After connecting to the system, a blank screen will appear.

Pressing any key will display the login screen shown below.

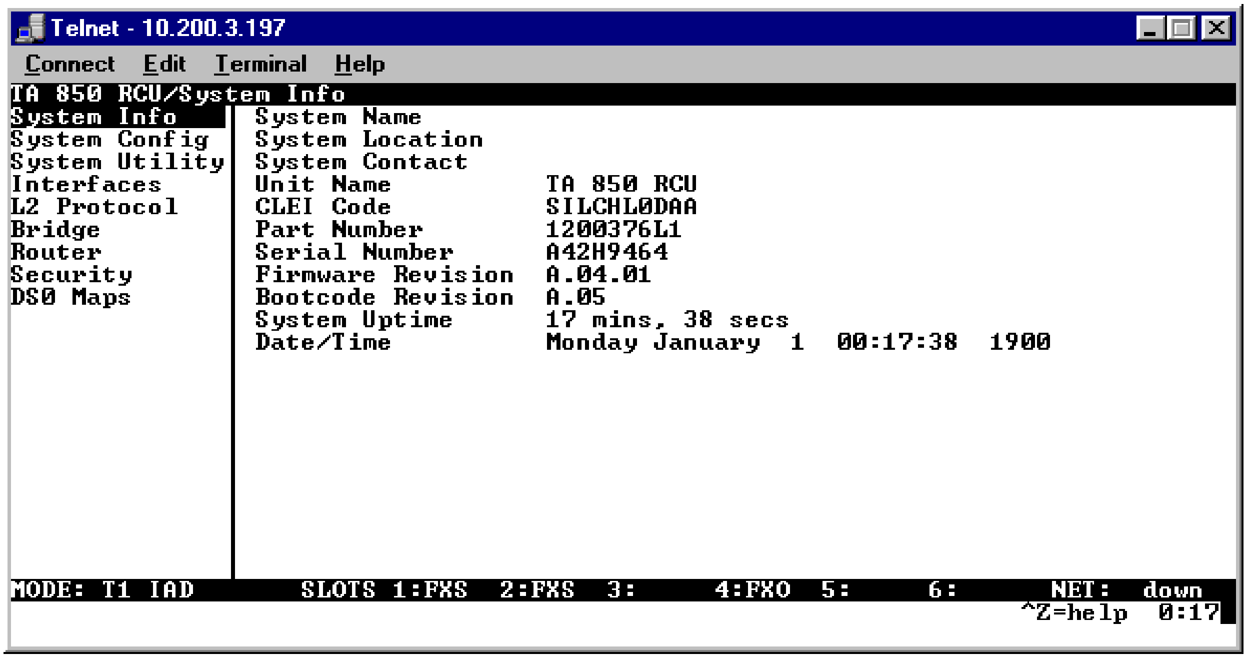


The cursor will blink at the **LOGIN** field, waiting for a password to be entered.

**2. At the LOGIN field, enter the password for the Total Access 850.**

Passwords to the Total Access 850 system are case sensitive. There is not a manufacturer's password by default. Press **<enter>** to enter the Total Access 850 menu.

3. **Upon entering the correct password, the Total Access 850 MAIN MENU is displayed as shown below.**



```
TA 850 RCU/System Info
System Info     System Name
System Config   System Location
System Utility  System Contact
Interfaces      Unit Name           TA 850 RCU
L2 Protocol     CLEI Code           SILCHL0DAA
Bridge          Part Number         1200376L1
Router          Serial Number       A42H9464
Security        Firmware Revision   A.04.01
DS0 Maps        Bootcode Revision   A.05
                System Uptime       17 mins, 38 secs
                Date/Time           Monday January  1  00:17:38  1900







MODE: T1 IAD      SLOTS 1:FXS  2:FXS  3:      4:FXO  5:      6:       NET:  down
                                                                ^Z=help  0:17
```

4. **You are now logged in to the Total Access 850 menu system.**

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# CONNECTING THE TERMINAL OR PC TO THE CRAFT PORT

### *Introduction*

Total Access  850 shelf management and provisioning is facilitated by a series of intuitive menus that are accessible on a computer screen. Connecting either a VT-100 terminal or a PC emulating a VT-100 terminal to the **CRAFT** port on the rear of the unit or the **CRAFT** interface on the RCU faceplate allows access to the menus and management features of Total Access  850. This section specifies how to connect the VT-100 terminal or PC to the Total Access  850.

The front **CRAFT** interface for the Total Access  850 is located on the faceplate of the RCU and is a DB-9 connector. Access can also be made to the Total Access  850 from the back of the unit through the port labeled **CRAFT**. It is an RJ-45 connector, and is located on the back of the unit. A special ADTRAN adapter is required for access to the RJ-45 craft port on the rear.

### *Prerequisite Procedures*

The Total Access  850 must be powered for terminal communication to function.

### *Tools and Materials Required*

- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access  850 (customer-provided)
- DB-9 male to DB-9 female serviceable (customer-provided) for connecting to the RCU **CRAFT** port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary.

**WARNING** *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

**CAUTION** *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.*

# DLP-005

**Perform Steps Below in the Order Listed**

1. Connect a VT-100 terminal to Total Access 850.

- Set the parameters of the VT-100 terminal to:
  - 9600 baud rate
  - 8 data bits
  - No parity
  - 1 stop bit
  - No flow control
- If the terminal has a parallel setting, disable it and use serial port.
- Plug the RJ-45 male end of the data cable into the CRAFT port on the rear of the Total Access 850, or plug the DB-9 connector into the faceplate of the RCU. Make the connection to the VT-100 terminal as appropriate for your equipment.

**2. Connect a PC emulating a VT-100 terminal to Total Access 850.**

Most personal computers or laptops can run communications software that will emulate a VT-100 terminal. Windows programs such as Terminal© or Hyperterminal© are two such examples in the Windows format. However, there are many other adequate, commercially available software packages which will allow your PC or laptop to emulate a VT-100 terminal. Certain configuration items must be set on a PC or laptop to act as a VT-100 terminal for the Total Access 850.

- Set the PC for direct connect on the appropriate com port (instead of dial-up connection).
- Set the parameters of the communications software to:
  - 9600 baud rate
  - 8 data bits
  - No parity
  - 1 stop bit
  - No flow control
- Plug the RJ-45 male end of the data cable into the CRAFT port on the rear of the Total Access 850, or plug the DB-9 connector into the faceplate of the RCU. Make connection to the PC or laptop as appropriate for your equipment.

**3. Press <Enter> or <Ctrl> <R> until Login menu appears on screen.**

You are now ready to login to Total Access 850, as described in *, Logging in to the System*.

NOTE *A VT 100 terminal program is provided with the ADTRAN Utilities.*

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# ADDING/REMOVING USERS
# AND CHANGING PASSWORD SECURITY LEVELS

### *Introduction*

All menu items in the Total Access 850 are protected by passwords of varying security levels. By assigning different passwords to different security levels, the Total Access 850 System Administrator can control which users can view or change various menu items. You can assign multiple passwords at the same access level. This way, different users with the same access privileges can have different passwords. This procedure details the steps which must be performed to add/remove user profiles and assign password security levels in the Total Access 850.

### *Tools and Materials Required*

- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access 850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU **CRAFT** port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary.
- Ethernet cable from 10BaseT port on Total Access 850 to hub (customer-provided)
- Use Ethernet crossover if going from Total Access 850 to PC

**WARNING** *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

**CAUTION** *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.*

# DLP-006

**Perform Steps Below in the Order Listed**

1. **Connect to the Total Access 850 using either the 10BASET or CRAFT interfaces.**

   If you are not already connected to the unit's **CRAFT** interface (either with a VT-100 compatible terminal or with a PC running VT-100 emulation software), follow the procedure in .

   Alternately, if the unit is part of a management cluster connected to the local network, you may use a PC connected to the network to Telnet into the unit. Use the procedures in DLP-005 and DLP-011 to connect to the **10BASET** interface.

2. **Log in to the unit.**

   Log in to the unit (see  for details).

3. **Go to the SYSTEM CONFIG SYSTEM CONFIG/MANAGEMENT/TELNET ACCESS menu and select the USER LIST menu and press <Enter>.**

4. **To add a new user profile and password, right arrow over to the right pane.**

5. **Give the new user profile a name by selecting the NAME field, pressing <Enter>, and typing the user defined name.**

6. **Personalize the password for the appropriate level by selecting the PASSWORD field, pressing <Enter>, then typing the desired password. You will have to type the new password again to confirm it.**

   Passwords for the Total Access 850 system are case sensitive. There is no default password for a new user (i.e., you can configure a user as blank with no password). The current password displays as a series of asterisks (********).

7. **Select the IDLE TIME field and press <Enter>. This field defines the amount of time in minutes the session may be idle before the user is logged off. The range is 1-255. The default value is 10.**

8. **Assign the password level by selecting the LEVEL field and choosing from the following level descriptions.**

The Total Access  850 contains six different password levels. The table below gives a brief description of each level.

| **Select level...** | **If you want the user to....** |
|---|---|
| Status | Have read-only permission for all menu items - **minimum rights** |
| Voice | Have read permission for all menu items and permission to use test commands |
| Router | Have access to all commands except passwords, flash download, authentication methods, interface configurations, and telnet security levels. |
| Config | Have access to all commands except passwords, flash download, authentication methods, and telnet security levels. |
| Support | Have access to all commands except passwords and telnet security levels. |
| Full | Have permission to edit every menu item, including creating and editing passwords -- **maximum rights** |
| Router Only | Have read access to all menu items and write access to only the router menu. |

NOTE *Only one telnet session can be active at a time.*

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# UPDATING THE FIRMWARE OF A TOTAL ACCESS 850 USING XMODEM

### *Introduction*

The Total Access 850 supports firmware updates via the ETHERNET port using either TFTP from a network server or the CRAFT interface using XMODEM. XMODEM is found in the VT 100 terminal application in the ADTRAN Utilities package and in most PC VT 100 communications software packages. This procedure outlines the steps for a successful firmware upgrade using the CRAFT interface and XMODEM software. Firmware may be obtained from the ADTRAN website at www.adtran.com. Select **Support** and then **Post-Sales Technical Support**.

### *Tools and Materials Required*

- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access 850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU CRAFT port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the CRAFT port on the rear of the unit. This adapter is ADTRAN proprietary
- ADTRAN-provided file containing upgraded code
- XMODEM software

| | |
|---|---|
| WARNING | *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.* |

| | |
|---|---|
| CAUTION | *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.* |

# DLP-007

## *Updating Firmware via the Dip Switch*

**Perform the Steps Below in the Order Listed**

1. Using a VT 100 terminal emulation communication software package which contains XMODEM protocol support, log in to TA 850. Set the transmit rate of the emulation software to 9600 baud.

> NOTE *Make certain that the communications software package being used has flow control turned off.*

2. **Remove the RCU module from the chassis and flip the SW1 dip switch to down or open (to the right of the unit if you are facing it).**

> NOTE *The dip switch is red and is located at the top edge of the card.*

> NOTE *Only the first two dipswitches on the RCU are used. With the first dip switch down (to the right of the unit if you are facing it), the unit boots up in a mode to update the firmware. With the second dip switch down, the unit factory defaults at startup.*

3. **Press Enter until a menu appears.**

> NOTE *To shorten transmit time, select the option from the menu to change the transmit rate to 115.2 baud or the highest rate supported by the terminal emulation software. If this transmit rate is changed, change emulation software properties to match this rate and disconnect and connect again. Press* Enter *again until the menu appears.*

4. **Choose option 1, BEGIN XMODEM DOWNLOAD NOW, from the menu to start the XMODEM file download.**

**5. Press Y at the START FLASH DOWNLOAD NOW prompt to continue with the XMODEM file transfer.**

> NOTE *When TA 850 is ready to receive the XMODEM upload, the menu screen will display* **Transmit Flash . . . download file now***. If this does not appear, please review the steps above for possible configuration errors.*

**6. From the terminal emulation software, begin the XMODEM upload by using the appropriate command sequence. (If necessary, refer to terminal emulation software documentation for help. Also, when specifying the filename, ensure that the file transferred is the one provided by ADTRAN. Otherwise, the update will not complete successfully.)**

> NOTE *Because XMODEM data is being transferred in-band through the menu interface, the VT 100 menus of TA 850 will be inoperable from the* **CRAFT** *port.*

**7. When the update has successfully completed, TRANSFER COMPLETE appears in the terminal window. If an error occurs during the update, an error message will display in the terminal window. If this occurs, return to Step 3 and attempt the update again. If the same error occurs, contact ADTRAN Technical Support.**

**8. After the TRANSFER COMPLETE message has been displayed, pull the RCU card again and return dip switch SW1 to the closed or off position. Reinsert the RCU module.**

**9. Change the emulation software properties to 9600 baud. Disconnect and connect to the unit at this transmit rate and continue configuring the unit as normal.**

> NOTE *It is suggested that a factory default be conducted after the unit is updated with new firmware.*

## *Updating Firmware via the Console Menus*

**Perform the Steps Below in the Order Listed**

1. Connect to the Total Access 850 using the RJ-45 CRAFT interface.

   If you are not already connected to the shelf’s **CRAFT** interface (either with a VT-100 compatible terminal or with a PC running VT-100 emulation software), follow the procedure in . Connecting to the **CRAFT** interface limits the upgrade procedure to XMODEM Only.

2. **Log in to the unit.**

   Log in to the unit using the read-write password (see  for details).

3. **Go to the SYSTEM UTILITY menu and select the UPGRADE FIRMWARE menu; press <Enter>.**

4. **Go to the TRANSFER METHOD menu and select XMODEM.**

5. **Select START TRANSFER to start the update process. Enter Y to confirm the upgrade.**

6. **From the terminal emulation software, begin the XMODEM upload by using the appropriate command sequence. If necessary, refer to the terminal emulation software documentation for help.**

   Also, when specifying the filename, ensure that the file transferred is the one provided by ADTRAN. Otherwise, the update will not complete successfully. This may take several minutes.

   Because XMODEM data is being transferred in-band through the menu interface, the VT-100 menus of the Total Access 850 will be inoperable from the **CRAFT** interface. You can cancel the update at any time within the terminal emulation software. (Please consult the documentation provided by the terminal emulation software to determine how to do this.)

7. **When the update process has successfully completed, the following messages will display:**

   **Verifying downloaded FLASH image...**

   **Erasing FLASH...**

   **Programming FLASH...**

   **FLASH programmed successfully.**

   The Total Access 850 will restart immediately and the user may then log back into the system.

   Alternately, if the unit is part of a management cluster connected to the local network, you may use a PC connected to the network to Telnet into the unit. By utilizing the **ETHERNET** port, the Total Access 850 may be quickly upgraded using TFTP, provided there is a TFTP server on the local network. The Total Access 850 ships with ADTRAN Utilities software, which includes a TFTP server. See DLP-008, *Updating the Firmware of a Total Access 850 using TFTP* for more details.

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# UPDATING THE FIRMWARE OF A TOTAL ACCESS 850 USING TFTP

### *Introduction*

The Total Access 850 supports firmware updates via the **10BASET** Ethernet port using either TFTP from a network server or the **CRAFT** interfaces using XMODEM. This DLP provides the steps to follow for a successful firmware upgrade using the **10BASET** ethernet port and a TFTP Server.

### *Tools and Materials Required*

- A TFTP Server accessible on the local network (A TFTP server is provided with the unit as part of the ADTRAN Utilities software.)
- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access 850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU **CRAFT** port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary.
- Ethernet cable from 10BaseT port on Total Access 850 to hub (customer-provided)
- Use Ethernet crossover if going from Total Access 850 to PC

| | |
|---|---|
| WARNING | *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.* |

| | |
|---|---|
| CAUTION | *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.* |

# DLP-008

**Perform Steps Below in the Order Listed**

1. Connect to the  Total Access 850 using the 10BASET interface.

   If you are not already connected to the unit’s **ETHERNET** port using Telnet client software, use the procedure in DLP-005, *Connecting the Terminal or PC to the CRAFT Port*, to connect to the unit.

2. **Log in to the unit.**

   Log in to the unit (see  for details).

3. **Verify the TFTP server is running on the network. The user may ping the TFTP server from the Total Access 850 to verify communication.**

> NOTE *A TFTP server ships as part of the ADTRAN utilities. If using ADTRAN utilities, choose* ***START > PROGRAMS > ADTRAN UTILITIES > TFTP SERVER*** *to start the server.*

4. **Download the firmware upgrade file to your computer.**

> NOTE *If using ADTRAN utilities, save the upgrade file to the “**ADTNUTIL**” directory on your hard drive.*

5. **Go to the SYSTEM UTILITY menu and select the UPDATE FIRMWARE menu; press <Enter>.**

6. **Go to the TRANSFER METHOD menu and select TFTP.**

7. **Set the TFTP SERVER ADDRESS to the IP address of the machine running the TFTP server program.**

> NOTE *If using ADTRAN utilities, this will be the IP address that appears in the* ***TFTP SERVER STATUS*** *window.*

8. **Enter the filename of the update file into the TFTP SERVER FILENAME field.**

**9. Select START TRANSFER to start the update process. Enter Y to confirm the upgrade.**

Prior to the start of the upgrade, the transfer status will display **IDLE**. During the TFTP upload process, various status messages display in **CURRENT UPDATE STATUS** to indicate progress. The following table describes these messages.

| Message | Meaning |
|---|---|
| **Transferring... [X KB]** | Indicates communication with the TFTP network server has been established and the update file is being transferred between the Total Access 850 and the TFTP network server. |
| **Flash Programmed Successfully** | The unit has been upgraded successfully. |
| **Loaded code**<br>**ver x.x.x**<br>**chksum = xxxx** | Unit displays the version and checksum of the upgraded code. |
| **Resetting ....** | Unit is power cycling. |
| **RECV Error** | Unit will display this message if server filename is incorrect. |
| **Can not start tftp client**<br>****Reload** | Unit will display this message if tftp server address is incorrect. |
| **Transfer aborted** | User has selected **ABORT TRANSFER**. |

**10. When the update process has successfully completed, FLASH PROGRAMMED SUCCESSFULLY will display briefly in the TRANSFER STATUS field. This will be followed by a LOADED CODE VER X.X.X CHKSUM = XXXX message. Finally the TRANSFER STATUS field will display RESETTING ...**

The Total Access 850 will restart immediately and resume operation. After giving the unit sufficient time to reboot, the user may telnet back into the unit and log in.

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# SAVING THE CURRENT CONFIGURATION
# OF A TOTAL ACCESS 850 USING TFTP

### *Introduction*

The Total Access 850 supports configuration transfers from the unit (via the **10BASET** Ethernet port) to a TFTP server located on the network. This DLP provides the steps to follow for a successful configuration transfer using the **10BASET** Ethernet port and a TFTP Server.

### *Tools and Materials Required*

- A PC with a Telnet client software
- A TFTP Server accessible on the local network (A TFTP server is provided with the unit as part of the ADTRAN Utilities software.)
- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access 850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU **CRAFT** port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary.
- Ethernet cable from 10BaseT port on Total Access 850 to hub (customer-provided)
- Use Ethernet crossover if going from Total Access 850 to PC.

> WARNING
>
> *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

> CAUTION
>
> *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.*

# DLP-009

**Perform Steps Below in the Order Listed**

1. Connect to the  Total Access 850 using the 10BASET interface.

   If you are not already connected to the unit's **10BASET** port using Telnet client software, use the procedure in DLP-011, *Connecting to the ATLAS 850 Using Telnet*, to connect to the unit.

2. **Log in to the unit.**

   Log in to the unit (see  for details).

3. **Verify the TFTP server is running on the network.**

> NOTE *A TFTP server ships as part of the ADTRAN utilities. If using ADTRAN utilities, choose* ***START > PROGRAMS > ADTRAN UTILITIES > TFTP SERVER*** *to start the server.*

4. **Go to the SYSTEM UTILITY menu and select the CONFIGURATION TRANSFER menu; press <Enter>.**

5. **Verify the TRANSFER METHOD is set to TFTP.**

6. **Set the TFTP SERVER IP ADDRESS to the IP address of the machine running the TFTP Server Program.**

> CAUTION *If you are using the ADTRAN TFTP server, the IP address displays in the* ***STATUS*** *field. For other TFTP servers, please refer to the appropriate documentation.*

7. **Change TFTP SERVER FILENAME to a unique filename. This will be the name of the configuration file saved to the remote server. An example filename would be ta850.cfg.**

   Some TFTP servers constrain the format of the filename depending on the operating system of the server. For example, a TFTP server running on a PC under Windows 3.1 may only permit 8.3 format filenames (8 characters, period and three extension characters).

**8. Select the SAVE CONFIG REMOTELY menu field and press <Enter>.**

Enter **Y** to confirm the request.

**9. View CURRENT TRANSFER STATUS to verify the progress of the current transfer. During a successful transfer, you will first see DOWNLOAD: COPYING INTERNAL CONFIG, and then DOWNLOAD IN PROGRESS....**

**10. When the transfer process has successfully completed, IDLE displays in the CURRENT TRANSFER STATUS field and DOWNLOAD COMPLETE displays in the PREVIOUS TRANSFER STATUS field.**

WARNING

*TFTP is **not** secure. No passwords are required for client access. Anyone can access files through the IP port on the server machine if they know the target filename.*

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# LOADING THE CURRENT CONFIGURATION OF A TOTAL ACCESS 850 USING TFTP

### *Introduction*

The Total Access 850 supports configuration uploads from a unit (via the **10BASET** Ethernet port) to a TFTP server located on the network. This DLP provides the steps to follow for a successful configuration upload using the **10BASET** Ethernet port and a TFTP Server.

### *Tools and Materials Required*

- A PC with a Telnet client software
- A TFTP Server accessible on the local network (A TFTP server is provided with the unit as part of the ADTRAN Utilities software.)
- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access 850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU **CRAFT** port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary.
- Ethernet cable from 10BaseT port on Total Access 850 to hub (customer-provided)
- Use Ethernet crossover if going from Total Access 850 to PC

| | |
|---|---|
| WARNING | *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.* |

| | |
|---|---|
| CAUTION | *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.* |

# DLP-010

**Perform Steps Below in the Order Listed**

1. **Connect to the Total Access 850 using the 10BASET interface.**

   If you are not already connected to the unit's **10BASET** port using Telnet client software, use the procedure in DLP-011, *Connecting to the ATLAS 850 Using Telnet* to connect to the unit.

2. **Log in to the unit.**

   Log in to the unit using at least a level 3 password (see and for details).

3. **Verify the TFTP server is running on the network.**

> NOTE *A TFTP server ships as part of the ADTRAN utilities. If using ADTRAN utilities, choose* ***START > PROGRAMS > ADTRAN UTILITIES > TFTP SERVER*** *to start the server.*

4. **Go to the SYSTEM UTILITY menu and select the CONFIGURATION TRANSFER menu, then press <Enter>.**

5. **Verify the TRANSFER METHOD is set to TFTP.**

6. **Set the TFTP SERVER IP ADDRESS to the IP address of the machine running the TFTP Server Program.**

> CAUTION *If you are using the ADTRAN TFTP server, the IP address displays in the* ***STATUS*** *field. For other TFTP servers, please refer to the appropriate documentation.*

7. **Change TFTP SERVER FILENAME to a unique filename including path. This will be the name of the configuration file retrieved from the remote server. An example filename would be ta850.cfg.**

   Some TFTP servers constrain the format of the filename depending on the operating system of the server. For example, a TFTP server running on a PC under Windows 3.1 may only permit 8.3 format filenames (8 characters, period and three extension characters).

8. **Select the LOAD AND USE CONFIG menu field and press <Enter>.**

   Enter **Y** to confirm the request.

9. **View CURRENT TRANSFER STATUS to verify the progress of the current upload.**

**10. When the upload process has successfully completed, IDLE displays in the CURRENT TRANSFER STATUS field and DOWNLOAD COMPLETE displays in the PREVIOUS TRANSFER STATUS field.**

WARNING

*The Total Access 850 system is rebooted immediately after a configuration is successfully loaded. Any online sessions will be terminated.*

**11. After an appropriate length of time, the user may telnet back into the unit.**

WARNING

*TFTP is **not** secure. No passwords are required for client access. Anyone can access files through the IP port on the server machine if they know the target file's name.*

### Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# CONNECTING TO THE ATLAS 850 USING TELNET

### *Introduction*

If the ATLAS 850 is part of a management cluster connected to the local network, you may use a PC connected to the network to Telnet into the unit. This procedure details the steps which must be performed to Telnet into the unit.

### *Prerequisite Procedures*

Complete DLP-002, Setting IP Parameters for the Total Access 850 and , Verifying Communications Over an IP LAN (steps 1 and 2 only).

### *Tools and Materials Required*

- Access to a PC or other computer connected to the LAN.
- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the ATLAS 850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU **CRAFT** port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary.
- Ethernet cable from 10BaseT port on Total Access 850 to hub (customer-provided)
- Use Ethernet crossover if going from Total Access 850 to PC

WARNING

*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION

*Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.*

# DLP-011

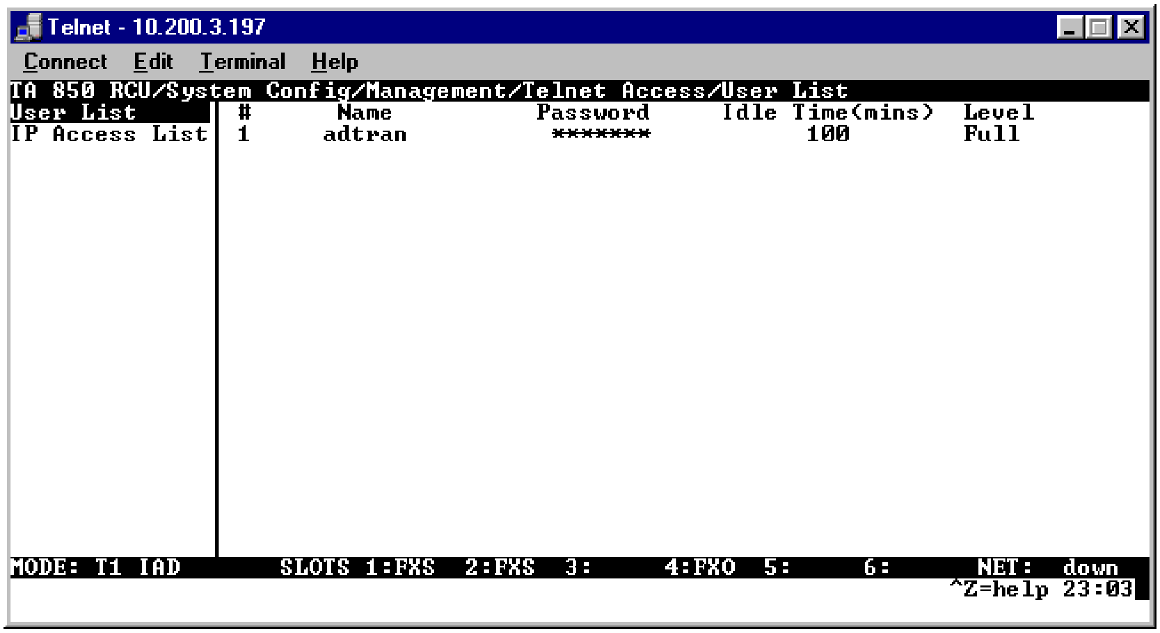
**Perform Steps Below in the Order Listed**

1. Connect the computer to the Total Access 850 **CRAFT** port as shown in .

**2. Log in to the unit as shown in .**

**3. Select the SYSTEM CONFIG/MANAGEMENT/TELNET ACCESS menu. Set the TELNET ACCESS to ON.**

**4. Under the SYSTEM CONFIG/MANAGEMENT/TELNET ACCESS menu, select the TELNET USER LIST; press <Enter>. The following screen will appear.**



```
TA 850 RCU/System Config/Management/Telnet Access/User List
User List       #      Name          Password      Idle Time(mins)   Level
IP Access List  1     adtran         ********            100         Full

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:    4:FXO  5:    6:     NET:  down
                                                            ^Z=help 23:03
```

**5. Use the right arrow key to select the NAME field; press <Enter>. Enter a username to be used for Telnet logins.**

**6. Use the right arrow key to select PASSWORD; press <Enter>. Enter a password to be used for Telnet logins.**

**7. Use the right arrow key to select IDLE TIME (MINS); press <Enter>. This field defines the amount of time in minutes the Telnet session may be idle before the user is logged off. The range is 1-255. The default value is 10 minutes. Enter the appropriate Idle Time.**

**8. Use the right arrow key to select LEVEL. Select the appropriate security level. Reference for security level definitions.**

**9. Press the left arrow key until prompted to save the Telnet changes. Type Y for yes.**

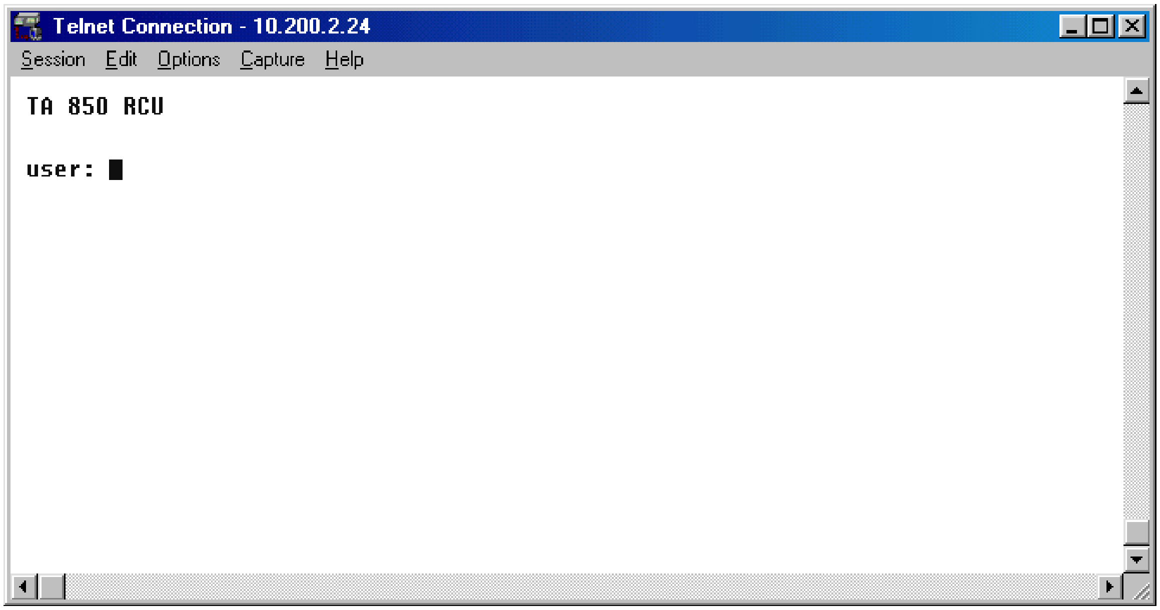
**10. This completes the addition of one Telnet user. Repeat steps 1-10 for each user needing Telnet access.**

**11. Press <Control L> to log out of the Total Access 850.**

**12. From a remote computer system connected to the LAN, Telnet to the Total Access 850.**

> NOTE
>
> *Refer to the documentation of the computer system if you are unsure how to perform a Telnet. Most computers running a networked version of Microsoft Windows™ or UNIX allow a Telnet to be performed by simply typing "Telnet <IP Address>" at a command line prompt. Telnet is a utility common on many local area networks that allows remote access to another computer or piece of equipment.*

The following screen will appear.

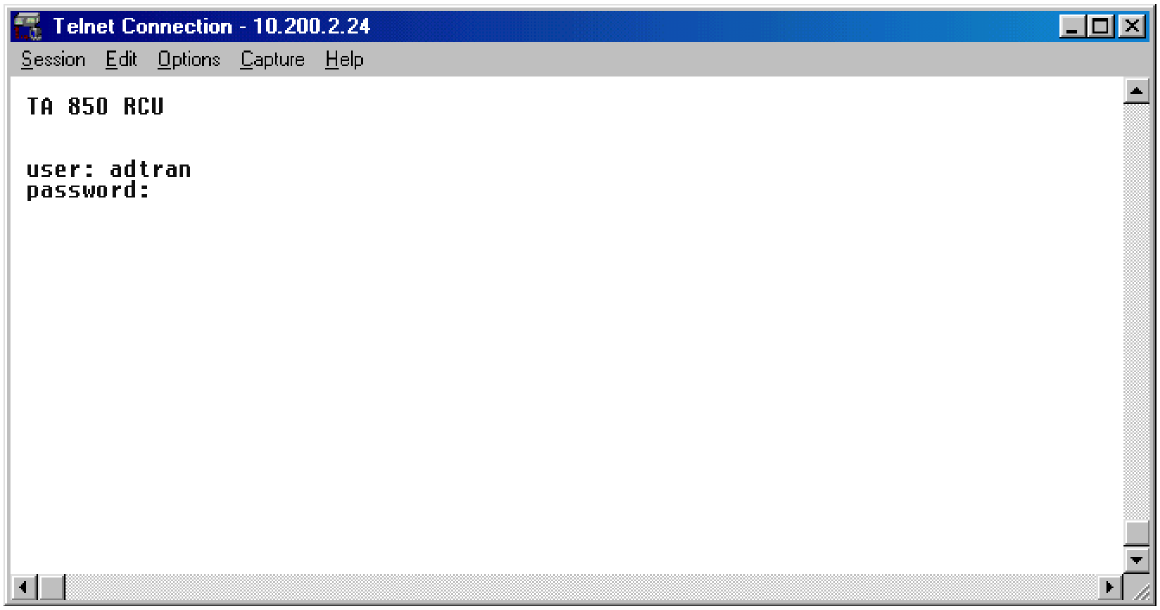

Telnet Connection - 10.200.2.24
Session Edit Options Capture Help

```
TA 850 RCU

user:
```

**13. Enter the user name assigned in step five and press enter.**

The following screen will appear.

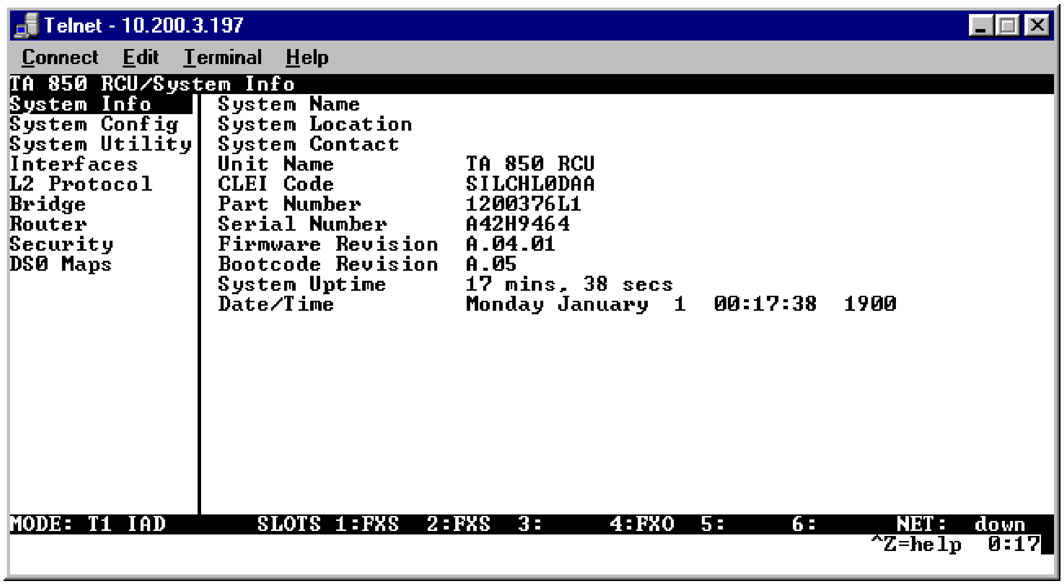

Telnet Connection - 10.200.2.24
Session Edit Options Capture Help

```
TA 850 RCU

user: adtran
password:
```

**14. Enter the password assigned in step 7.**

Upon entering the correct password, the Total Access 850 Main Menu is displayed as shown below:



```
TA 850 RCU/System Info
System Info     System Name
System Config   System Location
System Utility  System Contact
Interfaces      Unit Name          TA 850 RCU
L2 Protocol     CLEI Code          SILCHL0DAA
Bridge          Part Number        1200376L1
Router          Serial Number      A42H9464
Security        Firmware Revision  A.04.01
DS0 Maps        Bootcode Revision  A.05
                System Uptime      17 mins, 38 secs
                Date/Time          Monday January  1  00:17:38  1900

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:        NET:  down
                                                                  ^Z=help  0:17
```

You are now Telnetted into the Total Access 850 menu system.

**15. When you complete your configuration changes and save the changes (when prompted), press <Ctrl+L> to logout and close the session.**

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# SAVING AND LOADING TEXT CONFIGURATION USING TERMINAL COMMAND LINE

### *Introduction*

The Total Access 850 RCU has the ability to download a text file, which contains the configuration of the entire unit. This configuration may then be altered in a text editor, and then uploaded to that same or any other 850 RCU.

This DLP will explain how to save and load the configuration of the ADTRAN Total Access 850.

### *Prerequisite Procedures*

You must connect to the Total Access 850 with a VT100 terminal session (reference , *Connecting the Terminal or PC to the CRAFT Port* and , *Connect a PC emulating a VT-100 terminal to Total Access 850.*) or via a Telnet session (reference , *Verifying Communications Over an IP LAN* and *Telnet to the Total Access 850*).

### *Tools and Materials Required*

- Access to a PC or other computer connected to the LAN (Telnet access only)
- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Acess 850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU **CRAFT** port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary.
- Ethernet cable from 10BaseT port on Total Access 850 to hub (customer-provided)
- Use Ethernet crossover if going from Total Access 850 to PC

WARNING *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

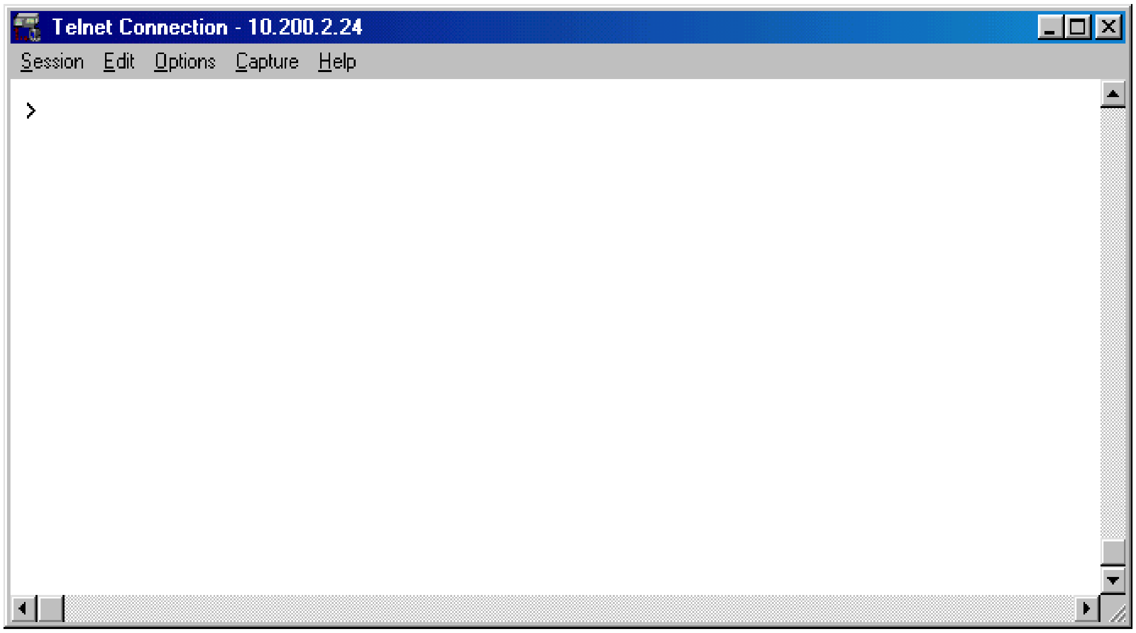
CAUTION *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.*

# DLP-012

**Perform Steps Below in the Order Listed**

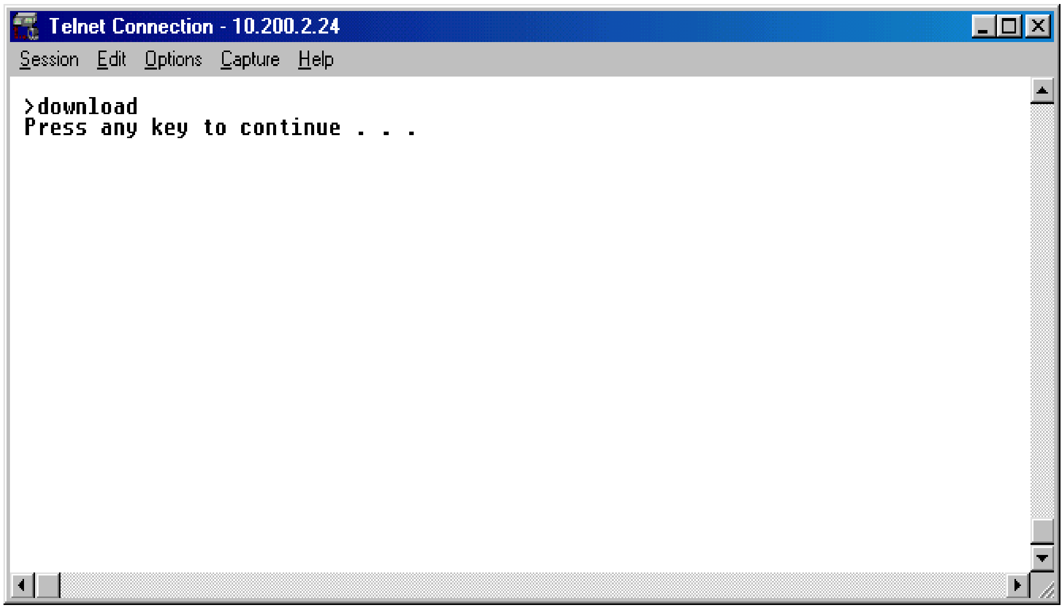
## Saving the router's configuration

1. **Establish a connection to the router with the terminal software either through the Maintenance Port or via a Telnet session.**
2. **From the Main Menu, select System Utility, then Terminal mode, then press ENTER.**
3. **The following screen will appear.**


Telnet Connection - 10.200.2.24
Session Edit Options Capture Help

```
>
```

4. **At the terminal prompt, type *download* and then press ENTER. The following screen will appear.**


Telnet Connection - 10.200.2.24
Session Edit Options Capture Help

```
>download
Press any key to continue . . .
```

5. **Don’t press another key yet!**

6. **Enable "capture" or "logging" in the terminal software, saving it to a file on your computer.**

7. **Press the SPACE BAR to continue. The router will then print its configuration to the terminal screen. (With capture enabled, the terminal software will capture the configuration and write it to the file that you designated.)**

8. **When the configuration stops printing, end the capture. The router's configuration is now saved to the file that you designated.**

9. **At the terminal prompt, type exit to go back into the configuration menu of the router.**

10. **Always use Ctrl+L to exit the configuration menu before closing the Telnet or terminal software.**

### Loading a configuration into the router

The following steps walk through uploading the text file back into the Total Access 850. These text files can be the entire configuration, or just partial commands that affect specific configuration changes. The uploading steps are the same, no matter of the size of the file.

1. **Establish a connection to the router with the terminal software either through the Maintenance Port or via a Telnet session.**
2. **From the Main Menu, select System Utility, then Terminal Mode, then press ENTER.**

3. **In the terminal software, initiate a SEND TEXT FILE or SEND CFG FILE using the saved configuration file.**

**4. Once the file transfer is complete, type SAVE to save the configuration in the unit. Then type exit to go back into the configuration menu of the router.**

**5. Always use Ctrl+L to exit the configuration menu before closing the Telnet or terminal software.**

### Entering commands at the command prompt

To do this manually from the prompt, precede each instruction with a ">". **After uploading, to apply and save changes, you must issue the command "save" from the prompt.** The command will apply ALL changes to the Total Access 850 (the same as escaping all the way out of the terminal menu). To do a save to flash only, but not apply the changes, you can go back to the menu system and hit Ctrl-W.

The commands are based on string comparisons with the menu system (with spaces replaced with underscores). This means that the config command will appear exactly as it appears in the RCU terminal menus. To change a configuration, type in the option desired exactly as it appears on the menu. For example, to change the T1 timing mode, the command line would read

```
>sysconfig t1_timing_mode network    or
>sysconfig t1_timing_mode internal   or
>sysconfig t1_timing_mode dsx-1.
```

### Follow-Up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# A.03 TO A.04 FIRMWARE UPGRADE

### Introduction

The Total Access line of Integrated Access Devices includes both the ATM and TDM versions of the Total Access 850. Until now, the Total Access TDM units have been running firmware version A.03.xx. Recently, A.04.xx has been released to support the TDM Total Access IADs. The development of A.04.xx code is a significant step in the evolution of the Total Access product line, as it allows all Total Access family members to share the same base code. This means that features and fixes are more easily implemented and are propagated across the product line.

The two possible A.03 to A.04 upgrade paths are described in this DLP.

CAUTION *The choice of upgrade path will determine whether the unit's configuration is saved.*

NOTE *Since the A.03 and A.04 firmware loads are significantly different, the text configuration files for the two revisions are also different. It is recommended that the customer save a text configuration file for both the A.03 revision (prior to the upgrade) and for the A.04 revision (after completion of the upgrade). Refer to DLP-009 and DLP-012 for further instructions on how to save the configuration.*

WARNING *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

## Prerequisite Procedures

Obtain the A.04 firmware and the A.03.90 (Transition Build) firmware from the ADTRAN website (http://www.ADTRAN.com).

> *For the Total Access 850 units, select* ***SUPPORT > POST-SALES TECHNICAL SUPPORT > FIRMWARE UPDATES > 612/616/624 TDM.***

If further assistance is required, contact ADTRAN Technical Support at 1-888-4ADTRAN.

## Tools and Materials Required

- VT100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the unit (customer-provided)
- DB-9 female to RJ-45 female adapter (customer provided) for connecting to the **CRAFT** port on the rear of the unit

# DLP-013

**Perform Steps Below in the Order Listed**

## Upgrade From A.03 to A.03.90 (Transition Build) to A.04

1. Upgrade the firmware from A.03 to A.03.90 (Transition Build) firmware. See DLP-007 or DLP-008 for instructions on how to perform this upgrade.
2. Once the upgrade to A.03.90 is complete, immediately upgrade the unit to A.04. See DLP-007 or DLP-008 for instructions on how to perform this upgrade.

> NOTE *Upgrading from A.03 to A.03.90 (Transition Build) to A.04 will save the unit's configuration.*

## Upgrade From A.03 to A.04 Directly

1. Upgrade the firmware from A.03 to A.04 firmware. See DLP-007 or DLP-008 for instructions on how to perform this upgrade.
2. The unit must then be factory defaulted by one of the following methods:
    - Select **SYSTEM UTILITY>TERMINAL MODE.** At the > prompt, type **fac**. You will then see “Restore Factory Defaults and Reset Unit? (press 'y').” Press the **y** key to confirm default. The unit will then automatically reset.
3. If connected to the **CRAFT** port, power reset the unit and then restore power to the unit while holding down the **F** key. You will then be prompted to confirm the factory default.
4. Reconfigure the unit for the specific application.

> NOTE *Upgrading from A.03 to A.04 directly (or from A.04 to A.03 directly) will erase the unit's configuration.*

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# CONFIGURING THE TOTAL ACCESS 850 FOR DUAL T1 MAPS

### *Introduction*

The Total Access 850 with firmware A.04.02 or higher has a **DUAL T1 MAP** feature that allows two network T1 connections for the termination of data and voice applications. The primary network **T1 MAP** can be configured for internal router usage (FT1/24 DS0s maximum) and to any access module installed. The **DSX MAP** can be used for FXS/FXO modules in slots 1-6 only. There are several steps that must be followed in order for the Dual T1 Map to be configured successfully. These steps are described in this DLP to ensure proper setup.

### *Prerequisite Procedures*

This procedure assumes that the user has access to the Total Access 850 system menus.

NOTE *Please see DLP-005 for assistance with making a terminal connection to the Total Access 850.*

### *Tools and Materials Required*

- VT-100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access 850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU **CRAFT** port
- DB-9 female to RJ-45 female adapter (customer-provided) for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary.

WARNING *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION *Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.*

# DLP-014

**Perform Steps Below in the Order Listed**

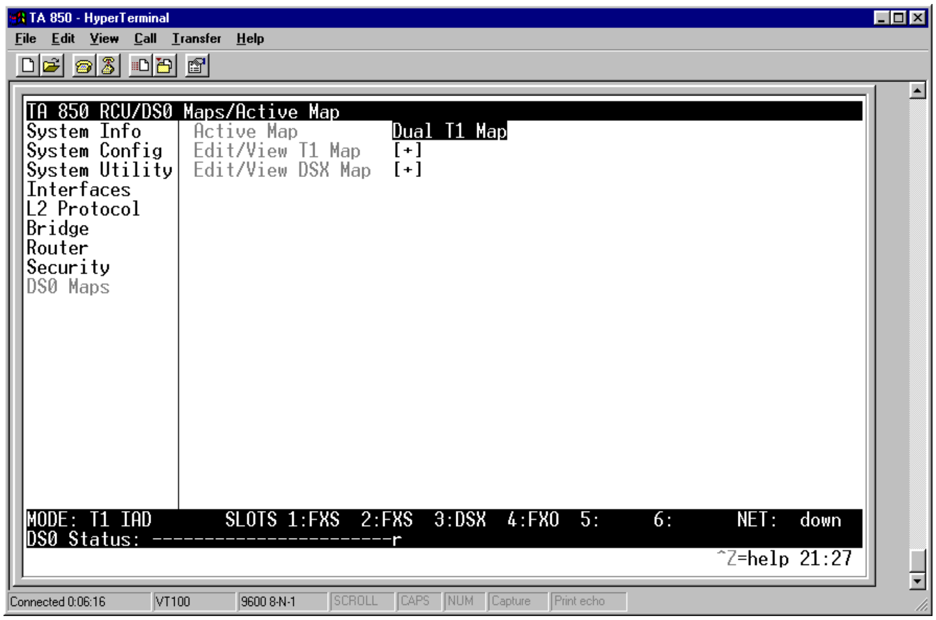
1. **Confirm the connection of the Total Access 850 unit to your VT-100 system (details found in DLP-005).**

2. **Log in to the system with maximum rights (details for logging in are in DLP-006).**

3. **From the DS0 Maps menu, select the Active Map option and press <Enter>.**

4. **From the DS0 Maps > Active Maps menu, select the Dual T1 Map option and press <Enter>. Select “Y” for yes to confirm the Active Map change and press <Enter>. The following screen will appear.**

> *The second T1 connected to the DSX port can only be used for voice connections (FXS/FXO). The second T1 must be connected to the integrated DSX port, not the DSX-1 Card.*

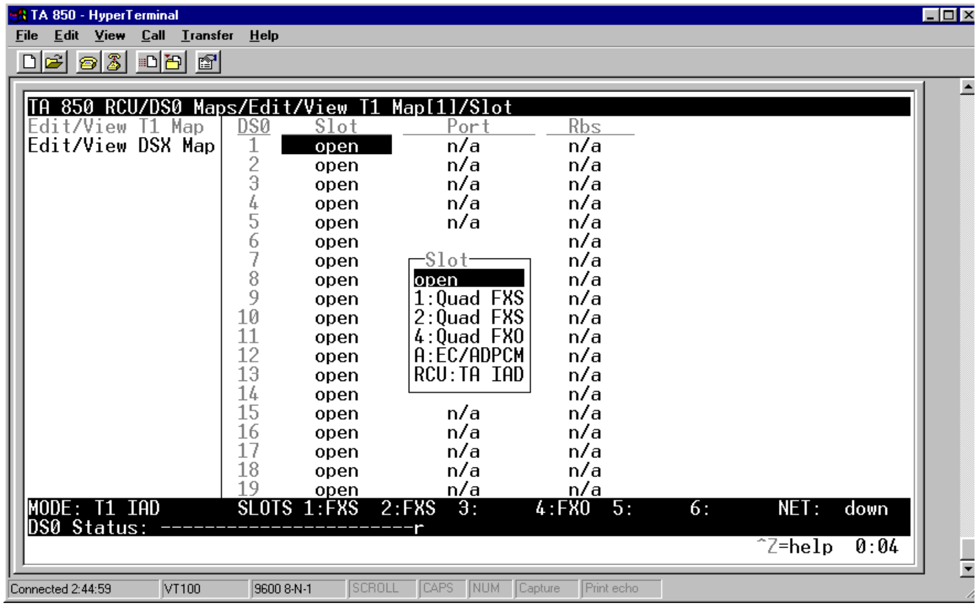


```
TA 850 RCU/DS0 Maps/Active Map
System Info      Active Map        Dual T1 Map
System Config    Edit/View T1 Map  [+]
System Utility   Edit/View DSX Map [+]
Interfaces
L2 Protocol
Bridge
Router
Security
DS0 Maps

MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:DSX  4:FXO  5:     6:       NET:  down
DS0 Status: -----------------------r
                                                                ^Z=help 21:27
```

Figure 1. Dual T1 Map

**5. Edit the Primary T1 Map by pressing <Enter> on EDIT/VIEW T1 MAP [+].The following screen will appear.**

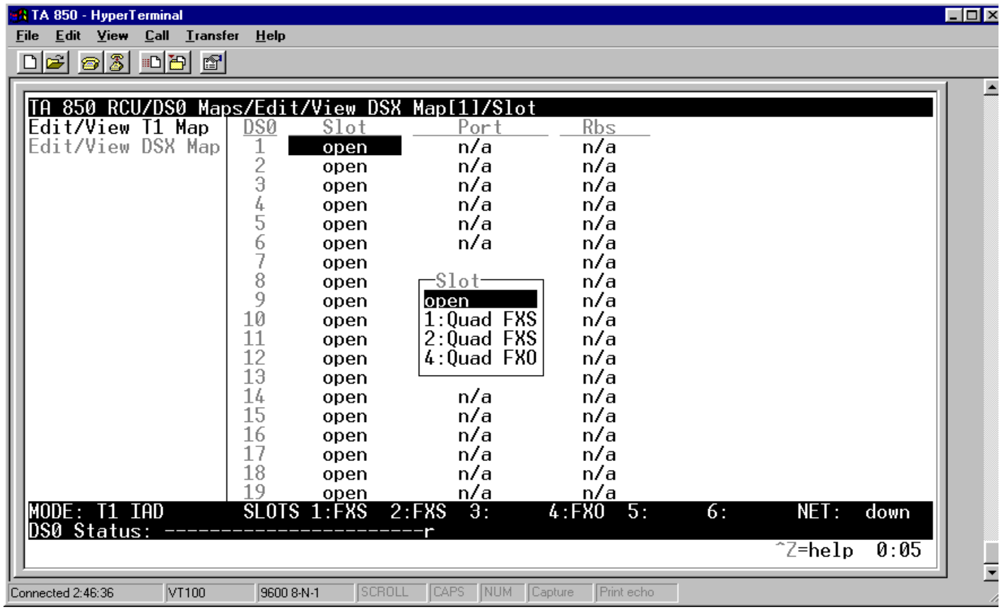


```
TA 850 RCU/DS0 Maps/Edit/View T1 Map[1]/Slot
Edit/View T1 Map  DS0    Slot        Port        Rbs
Edit/View DSX Map  1     open        n/a         n/a
                   2     open        n/a         n/a
                   3     open        n/a         n/a
                   4     open        n/a         n/a
                   5     open        n/a         n/a
                   6     open                    n/a
                   7     open     ┌Slot─────────┐n/a
                   8     open     │open         │n/a
                   9     open     │1:Quad FXS   │n/a
                   10    open     │2:Quad FXS   │n/a
                   11    open     │4:Quad FXO   │n/a
                   12    open     │A:EC/ADPCM   │n/a
                   13    open     │RCU:TA IAD   │n/a
                   14    open     └─────────────┘n/a
                   15    open        n/a         n/a
                   16    open        n/a         n/a
                   17    open        n/a         n/a
                   18    open        n/a         n/a
                   19    open        n/a         n/a
MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:       NET:  down
DS0 Status: -----------------------r
                                                               ^Z=help  0:04
```

Figure 2. Primary T1 Map

NOTE *The T1 Map can be mapped to the internal router or other available access module.*

6. **Edit the Secondary T1 Map (DSX Map) by pressing <Enter> on EDIT/VIEW DSX MAP [+]. The following screen will appear.**



```
TA 850 RCU/DS0 Maps/Edit/View DSX Map[1]/Slot
Edit/View T1 Map   DS0    Slot        Port        Rbs
Edit/View DSX Map   1     open        n/a         n/a
                    2     open        n/a         n/a
                    3     open        n/a         n/a
                    4     open        n/a         n/a
                    5     open        n/a         n/a
                    6     open        n/a         n/a
                    7     open                    n/a
                    8     open     ┌Slot──────┐   n/a
                    9     open     │open      │   n/a
                    10    open     │1:Quad FXS│   n/a
                    11    open     │2:Quad FXS│   n/a
                    12    open     │4:Quad FXO│   n/a
                    13    open     └──────────┘   n/a
                    14    open        n/a         n/a
                    15    open        n/a         n/a
                    16    open        n/a         n/a
                    17    open        n/a         n/a
                    18    open        n/a         n/a
                    19    open        n/a         n/a
MODE: T1 IAD        SLOTS 1:FXS  2:FXS  3:     4:FXO  5:     6:      NET:  down
DS0 Status: -----------------------r
                                                            ^Z=help  0:05
```

**Figure 3. DSX Map**

NOTE *The DSX Map can be mapped to the FXS and FXO access modules only.*

7. **Left arrow back to DS0 MAPS. Log off by pressing <Ctrl+L>.**

### *Follow-up Procedures*

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

# ADTRAN UTILITIES

ADTRAN delivers several PC software utilities along with the unit. These utilities are located on the CD-ROM that came with your shipment. They also include MIB files (located in the MIB directory).

NOTE *Review the readme file (Readme.txt) for the latest information about the utilities.*

The utilities make it easier to interface with the terminal menu and transfer configuration files to and from TFTP servers. The utilities all run on Microsoft Windows 3.1 or higher. The following sections describe the Telnet, VT100, and TFTP Server utilities.

## CONTENTS

## FIGURES

NOTE *In this section, unit refers to the Total Access 850.*

## 1. TELNET UTILITY

The Telnet utility delivered with the unit provides enhancements to standard Telnet programs that make it easier to work with unit options.

Access the Telnet program remotely through the **10/100BaseT** Ethernet port. For a detailed description of how to work with the Telnet program, refer to *Navigating the Terminal Menus* in the Commons User Interface Guide section of this manual. If you need help setting up the unit for a Telnet session, refer to the Detailed Level Procedures section of this manual.

The Telnet menus include **Session**, **Edit**, **Options**, **Capture**, and **Help** (see the menu tree in Figure 1).

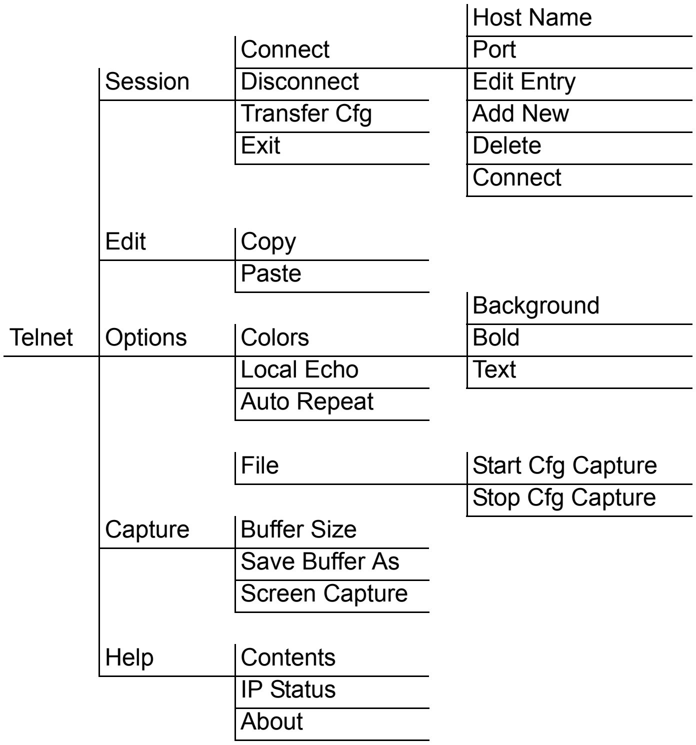


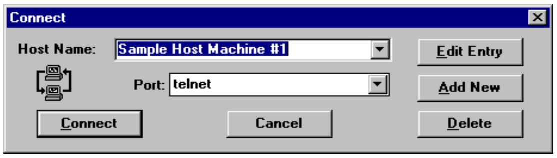
**Figure 1. Telnet Menu Tree**

### *Session Menu*

Click on **Session** to open the Telnet session.

### Connect

Opens dialog box for setting **Host Name** and **Port** parameters for a Telnet session. Also lets you **Edit Entry**, **Add New** entry, and **Delete** stored entries. When the parameters are set, click **Connect** to make the connection. Click **Cancel** to end the session.



Host Name: Sample Host Machine #1
Port: telnet

#### *Host Name*

Accepts and stores host names. You may either enter a name, an IP address, or a domain name directly from this field. Click on the drop-down arrow to display a complete list of previously stored host names.

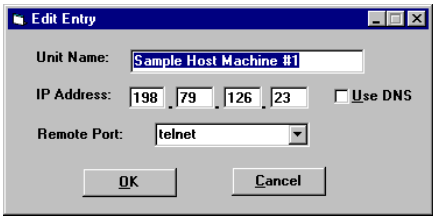
#### *Port*

Provides several port options. You may enter port numbers directly into this field to connect to non-standard ports or select the drop-down combo-box to display the following options:

| | |
|---|---|
| **Telnet** | establishes a Telnet session |
| **Echo** | provides a loopback for troubleshooting |
| **Discard** | bit bucket; discards data |
| **Daytime** | returns the time |
| **Chargen** | displays as a unique character stream; used for self-tests |

#### *Edit Entry*

Changes either the unit name or the IP address of each host. Press either **Tab, Return,** or a **period (.)** after each number in the IP address to move to the next field. If you press **Return** or **(.)** while the cursor is located in each IP field, that field entry is deleted.



Unit Name: Sample Host Machine #1
IP Address: 198 . 79 . 126 . 23
□ Use DNS
Remote Port: telnet

#### *Add New*

Prompts you for the same information as the **Edit Entry** dialog box for new host. When enabled, the **Use DNS** (Domain Name Server) feature allows users to request **Domain Look Up** via a DNS server on the network, rather than specifying an IP address. The name then appears in the **Host Name** field.

#### *Delete*

Removes a host name from the list; simply select the host name you want to remove, and, at the prompt, click **Delete**.

#### *Connect*

Establishes the Telnet session.

### Disconnect

Terminates the Telnet session.

To re-establish the session, select **Connect** from **Session Menu** or press **Enter** three times. This action restores the previous connection.

### Transfer Cfg

This feature is used with ADTRAN products primarily for sending configuration files to the unit.

### Exit

Ends the Telnet session and closes the Telnet screen.

## *Edit Menu*

Provides **COPY** and **PASTE** commands.

## *Options Menu*

Provides viewing alternatives for the terminal screen.

### Colors

Three options change the color of the background window (**BACKGROUND**), bold highlights (**BOLD**), and text (**TEXT**).

### Local Echo

Echoes each character that you enter.

### AutoRepeat

Repeats characters you select from the keyboard, if you hold down the key.

## *Capture Menu*

Provides options for capturing screen images.

### File

Sends screen options data to a file in the format options listed below:

#### *Start Cfg Capture*

Used with the ADTRAN product line to start sending the scrolling screen capture to a file storage location.

#### *Stop Cfg Capture*

Used with the ADTRAN product line to stop sending the scrolling screen capture to a file storage location.

### Buffer Size

Disables terminal window scroll bars when set to zero. This is the normal setting. This number represents the number of lines to capture in the memory buffer.

### Save Buffer As

Save screen capture to a file.

### Screen Capture

Copies the text on the current Telnet screen to the clipboard. You can open any word processor and paste the clipboard contents into the program. This option is helpful when debugging.

### *Help Menu*

Provides on-line help for using the ADTRAN Utilities.

**Contents**
Opens the on-line help.

**IP Status**
Displays the local port address and the status of the connection.

**About**
Displays version and owner information.

## 2. VT100 UTILITY

Use the VT100 to configure a unit which is directly connected to a PC. The VT100 display is almost identical to the Telnet display.

For a detailed description of how to work within the terminal menu, refer to *Navigating the Terminal Menus* in the User Interface Guide section of this manual. If you need help setting up the unit for a VT100 session, refer to the Detailed Level Procedures section of this manual.

VT100 menus include **SESSION**, **EDIT**, **PORT**, **OPTIONS**, **CAPTURE**, and **HELP** (see the menu tree in Figure 2).

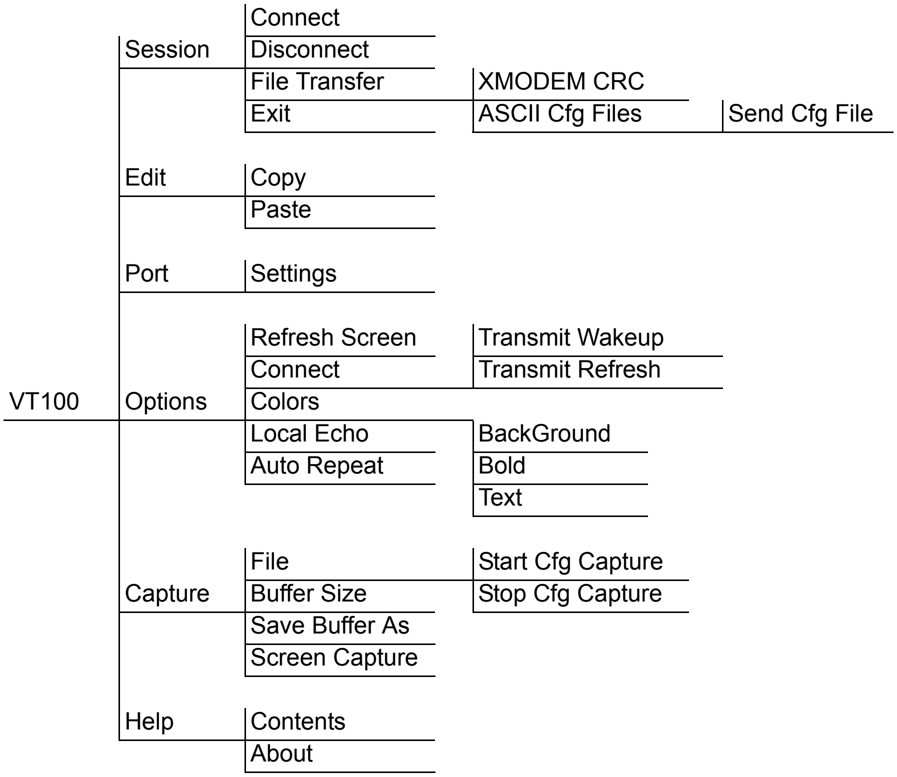


**Figure 2. VT100 Menu Tree**

## *Session Menu*

Opens VT100 terminal emulation session.

### Connect

Opens a specified serial port for a VT100 session.

### Disconnect

Closes a specified serial port at the end of a VT100 session.

### File Transfer

Uploads and downloads files to and from the unit.

#### *XMODEM CRC*

Selects the XMODEM file transfer protocol.

#### *ASCII Cfg Files*

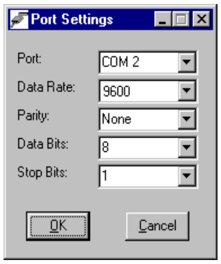
Selects ASCII transfer mode. Primarily useful for configuration transfers for the ADTRAN products.

## *Edit Menu*

Identical to the Telnet **Edit Menu** (see *Edit Menu* on page 354).

## *Port Menu*

Changes serial COM port **Settings**. Provides data rate settings from 300—57600 bps.



Port Settings

Port: COM 2

Data Rate: 9600

Parity: None

Data Bits: 8

Stop Bits: 1

## *Options Menu*

Provides terminal screen commands.

### Refresh Screen

Redraws the screen.

### Connect

Provides the options **Transmit Wakeup** and **Transmit Refresh**.

#### *Transmit Wakeup*

Provides a control sequence that puts the unit **Craft** port online in terminal mode.

#### *Transmit Refresh*

Provides a control sequence to refresh the screen automatically when connecting. This is the default setting.

### Colors

Identical to Telnet **Colors Menu** (see *Colors* on page 354).

### Local Echo

Echoes each character that you enter.

**AutoRepeat**
Repeats characters you select from the keyboard if you hold down the key.

### *Capture Menu*

Identical to the Telnet **CAPTURE MENU** (see *Capture Menu* on page 354).

### *Help Menu*

Provides on-line help and information about the version number.

**Contents**
Opens on-line help.

**About**
Displays version and owner information.

## 3. TFTP SERVER

The TFTP Server utility transfers configuration files to and from a TFTP server. You can install this program on a PC running any version of Microsoft Windows. The configuration of the unit can be saved offline as a backup file. The saved file may also be used to send the same configuration to multiple units. Transfer configuration files using the TFTP protocol (a TCP/IP user protocol) via the **10/100BASET** Ethernet port. The unit must have a valid IP address, subnet mask, and default gateway (if required), and be connected to an Ethernet network before proceeding. Figure 4 shows the TFTP server interface. For information on transferring and saving configurations using TFTP, refer to the Detailed Level Procedures section of this manual.

NOTE *Files must be placed in the Application directory where you installed the product. Received files are also placed here.*

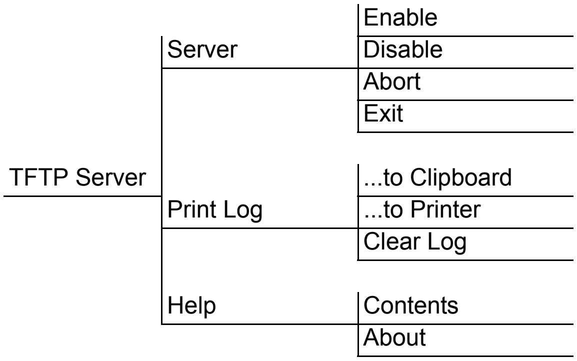
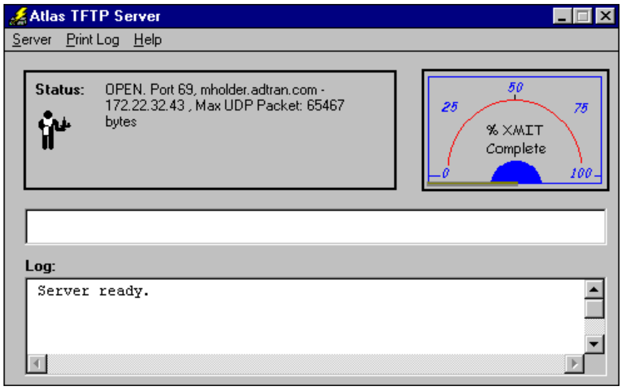


**Figure 3. TFTP Server Interface Menu Tree**



Status: OPEN. Port 69, mholder.adtran.com - 172.22.32.43 , Max UDP Packet: 65467 bytes

Log:

```
Server ready.
```

**Figure 4. TFTP Server Interface**

Only one configuration transfer session (upload or download) may be active at a time. The TCP/IP parameters are not saved or overwritten as part of the unit's transferred configuration to allow sending identical configurations to multiple units. When you start this program, a port is automatically opened.

## *Server Menu*

Provides enable, disable, abort, and exit options.

### Enable

Enables the TFTP server. The IP address displays in the Status field and Server Ready displays in the Log field.

### Disable

Disables the TFTP server. When you select this option, the message PORT CLOSED displays in the Status field and Port Closed displays in the Log field.

### Abort

Terminates a transfer that is in progress.

### Exit

Terminates active transfers and closes the TFTP window.

## *Print Log*

Provides print options.

### ...to Clipboard

Copies the information in the Log field to the clipboard. You can then open any word processor and paste the information into the program for review.

### ...to Printer

Sends the information in the Log field to the default printer.

### Clear Log

Deletes the information stored in the Log field.

### *Help*

Provides on-line help and version information.

#### Contents

Opens on-line help.

#### About

Displays version and owner information.

## 4. STATUS FIELD

This field displays general information about port and transfer status. This field is read-only. The unlabeled field in the center of the screen displays prompts about the status of active transfers, such as bytes transferred and received.

## 5. METER FIELD

The **XMIT** meter provides a visual record of the transfer process.

## 6. LOG FIELD

This field displays a record of all of the events that occur during the time the TFTP Server is enabled. Use the scroll bar to move up and down the list. To clear the information in this field, select **CLEAR LOG** from the **PRINT LOG** menu. Save this information to a file before deleting it with the **...TO CLIPBOARD** command.

# MIB

This section is divided into two parts: (1) SNMP information for TDM units and (2) SNMP information for ATM units. Each section details the Management Information Bases (MIBs) supported, MIB Compilation Order, Traps Supported, and MIB Variables supported.

## CONTENTS

NOTE *For this section, TDM units refers to ATLAS 850 units running A.04 firmware or later. ATM units refers to ATLAS 850 units running C.02 firmware or previous.*

NOTE *The TDM units support SNMP Version 2.*
*The ATM units support SNMP Version 1.*

# 1. MIBs SUPPORTED BY TDM UNITS

**Standard RFC MIBs:**

| | |
|---|---|
| RFC1573.mi2 | IANAifType-MIB |
| RFC1907.mi2 | SNMPv2-MIB |
| RFC2011.mi2 | IP-MIB |
| RFC2096.mi2 | IP-FORWARD-MIB |
| RFC2115.mi2 | FRAME-RELAY-DTE-MIB |
| RFC2493.mi2 | PerfHist-TC-MIB |
| RFC2494.mi2 | DS0-MIB and DS0BUNDLE-MIB |
| RFC2495.mi2 | DS1-MIB |
| RFC2665.mi2 | EtherLike-MIB |
| RFC2863.mi2 | IF-MIB |
| RFC3201.mi2 | CIRCUIT-IF-MIB |

**Enterprise MIBs:**

| | |
|---|---|
| adtran.mi2 | ADTRAN-MIB |
| adIadSys.mi2 | ADTRAN-ADIADSYS-MIB |
| adIadRtr.mi2 | ADTRAN-ADIADROUTER-MIB |
| adIadVoi.mi2 | ADTRAN-ADIADVOICE-MIB |

NOTE *SNMPv2-SMI, SNMPv2-TC, SNMPv2-TM, SNMPv2-CONF should be included with the SNMP manager.*

NOTE *All TDM MIBs are SNMPv2*

## 2. MIB COMPILATION ORDER FOR TDM UNITS

IANAifType-MIB

PerfHist-TC-MIB

SNMPv2-MIB (if not included with SNMP manager)

IF-MIB

IP-MIB

IP-FORWARD-MIB

FRAME-RELAY-DTE-MIB

DS1-MIB

DS0-MIB

DS0BUNDLE-MIB

EtherLike-MIB

CIRCUIT-IF-MIB

ADTRAN-MIB

ADTRAN-IADSYS-MIB

ADTRAN-IADROUTER-MIB

## 3. TRAPS SUPPORTED BY TDM UNITS

| | |
|---|---|
| From RFC1215-MIB: | coldStart<br>linkDown<br>linkUp<br>authenticationFailure |

| | |
|---|---|
| From ADTRAN-IADSYS-MIB: | adIadWanDown - 1003203<br>adIadWanUp - 1003204<br>adIadBatteryAlarmAct - 1003207<br>adIadBatteryAlarmDeact - 1003208 |
| (T1 WAN interface only): | adIadDs1RedAlarmON - 1003209<br>adIadDs1YellowAlarmON - 1003210<br>adIadDs1BlueAlarmON - 1003211<br>adIadDs1RedAlarmOFF - 1003212<br>adIadDs1YellowAlarmOFF - 1003213<br>adIadDs1BlueAlarmOFF - 1003214<br>adIadDs1SEF - 1003215<br>adIadDs1FS - 1003216<br>adIadDs1CRC - 1003217<br>adIadDs1LCV - 1003218<br>adIadDs1SLP - 1003219 |
| From ADTRAN-IADVOICE-MIB: | adIadVoiceTestStatusActive - 1003401<br>adIadVoiceTestStatusClear - 1003402<br>adIadVoiceAlarmBitActive - 1003403<br>adIadVoiceAlarmBitInactive - 1003404<br>adIadVoiceGatewayDown - 1003405<br>adIadVoiceGatewayUp - 1003406<br>adIadVoiceaLifeLineActivated - 1003407<br>adIadVoiceaLifeLineDeactivated - 1003408 |

## 4. MIB VARIABLES SUPPORTED BY TDM UNITS

SNMPv2 states the supported MIB variables by the following method:

The unit will have a MIB called TA 6XX.mi2 that will describe what SNMP variables are supported. This MIB will contain an AGENT-CAPABILITIES MODULE that will describe the SNMP variables supported.

## 5. MIBs SUPPORTED BY ATM UNITS

**Standard RFC MIBs:**

| | |
|---|---|
| RFC1213.mib | RFC1213-MIB |
| RFC1406.mib | DS1-MIB (T1 interface only) |
| RFC1695.mib | ATM-MIB |

**Enterprise MIBs:**

| | |
|---|---|
| Adtran.mib | ADTRAN-MIB |
| adtartr_trap.mib | ADTRAN-ADTARTR_TRAP-MIB |

*RFC1155-SMI, RFC1212-MIB, and RFC1215-MIB are also needed and should come standard with any SNMP Management software.*

*All ATM MIBs are SNMPv1.*

## 6. MIB COMPILATION ORDER FOR ATM UNITS

RFC1213-MIB

RFC1406-MIB

RFC1695-MIB

ADTRAN-MIB

ADTRAN-ADTARTR-TRAP-MIB

## 7. TRAPS SUPPORTED BY ATM UNITS

| | |
|---|---|
| From ADTARTR_TRAP MIB: | coldStart<br>linkUp<br>linkDown<br>authenticationFailure<br>adTARouterWanDown - 6645503<br>adTARouterWanUp - 6645504<br>adTARouterBatteryAlarmAct - 6645507<br>adTARouterBatteryAlarmDeact - 6645508<br>adTARouterVoiceGatewayDown - 6645509<br>adTARouterVoiceGatewayUp - 6645510<br>adTARouterLifeLineActivated - 6645511<br>adTARouterLifeLineDeactivated - 6645512 |

## 8. MIB VARIABLES SUPPORTED BY ATM UNITS

NOTE *ATM units do not support write access for SNMP (except for sysName, sysLocation, and sysContact.*

| **system:** | |
|---|---|
| sysDescr | RO |
| sysObjectID | RO |
| sysUpTime | RO |
| sysContact | RW |
| sysName | RW |
| sysLocation | RW |
| sysServices | RO |

**interfaces:**

| | |
|---|---|
| ifIndex | RO |
| ifDescr | RO |
| ifType | RO |
| ifMtu | RO |
| ifSpeed | RO |
| ifPhysAddress | RO |
| ifOperStatus | RO |
| ifInOctets | RO |
| ifInUcastPkts | RO |
| ifInNUcastPkts | RO |
| ifInDiscards | RO |
| ifInErrors | RO |
| ifInUnknownProtos | RO |
| ifOutOctets | RO |
| ifOutUcastPkts | RO |
| ifOutNUcastPkts | RO |
| ifOutDiscards | RO |
| ifOutErrors | RO |
| ifSpecific | RO |

**ip:**

| | |
|---|---|
| ipForwarding | RO |
| ipDefaultTTL | RO |
| ipInReceives | RO |
| ipInHdrErrors | RO |
| ipInAddrErrors | RO |
| ipForwDatagrams | RO |
| ipInUnknownProtos | RO |
| ipInDiscards | RO |
| ipInDelivers | RO |
| ipOutRequests | RO |
| ipOutDiscards | RO |
| ipOutNoRoutes | RO |
| ipReasmOKs | RO |
| ipReasmFails | RO |
| ipFragOKs | RO |
| ipFragFails | RO |
| ipFragCreates | RO |

**ipAddrTable:**

| | | |
|---|---|---|
| ipAddrEntry | | |
| | ipAdEntAddr | RO |
| | ipAdEntIfIndex | RO |
| | ipAdEntNetMask | RO |
| | ipAdEntBcastAddr | RO |
| | ipAdEntReasmMaxSize | RO |

**ipRouteTable:**

ipRouteEntry

| | |
|---|---|
| ipRouteDest | RO |
| ipRouteIfIndex | RO |
| ipRouteMetric1 | RO |
| ipRouteMetric2 | RO |
| ipRouteMetric3 | RO |
| ipRouteMetric4 | RO |
| ipRouteNextHop | RO |
| ipRouteType | RO |
| ipRouteProto | RO |
| ipRouteAge | RO |
| ipRouteMask | RO |
| ipRouteMetric5 | RO |
| ipRouteMetricInfo | RO |

**ipNetToMediaTable:**

ipNetToMediaEntry

| | |
|---|---|
| ipNetToMediaIfIndex | RO |
| ipNetToMediaPhysAddress | RO |
| ipNetToMediaNetAddress | RO |
| ipNetToMediaType | RO |
| ipRoutingDiscards | RO |

**icmp:**

| | |
|---|---|
| icmpInMsgs | RO |
| icmpInErrors | RO |
| icmpInDestUnreachs | RO |
| icmpInTimeExcds | RO |
| icmpInParmProbs | RO |
| icmpInSrcQuenchs | RO |

| | |
|---|---|
| icmpInRedirects | RO |
| icmpInEchos | RO |
| icmpInEchoReps | RO |
| icmpInTimestamps | RO |
| icmpInTimestampReps | RO |
| icmpInAddrMasks | RO |
| icmpInAddrMaskReps | RO |
| icmpOutMsgs | RO |
| icmpOutErrors | RO |
| icmpOutDestUnreachs | RO |
| icmpOutTimeExcds | RO |
| icmpOutParmProbs | RO |
| icmpOutSrcQuenchs | RO |
| icmpOutRedirects | RO |
| icmpOutEchos | RO |
| icmpOutEchoReps | RO |
| icmpOutTimestamps | RO |
| icmpOutTimestampReps | RO |
| icmpOutAddrMasks | RO |
| icmpOutAddrMaskReps | RO |

**tcp:**

| | |
|---|---|
| tcpRtoAlgorithm | RO |
| tcpRtoMin | RO |
| tcpRtoMax | RO |
| tcpMaxConns | RO |
| tcpActiveOpens | RO |
| tcpPassiveOpens | RO |
| tcpAttemptFails | RO |
| tcpEstabResets | RO |

| | | | |
|---|---|---|---|
| tcpCurrEstab | RO | | |
| tcpInSegs | RO | | |
| tcpOutSegs | RO | | |
| tcpRetransSegs | RO | | |
| | | | |
| tcpConnTable | | | |
| tcpConnEntry | | | |
| | | tcpConnState | RO |
| | | tcpConnLocalAddress | RO |
| | | tcpConnLocalPort | RO |
| | | tcpConnRemAddress | RO |
| | | tcpConnRemPort | RO |
| tcpInErrs | RO | | |
| tcpOutRsts | RO | | |

**udp:**

| | | | |
|---|---|---|---|
| udpInDatagrams | RO | | |
| udpNoPorts | RO | | |
| udpInErrors | RO | | |
| udpOutDatagrams | RO | | |
| udpLocalAddress | RO | | |
| udpLocalPort | RO | | |
| | | | |
| udpTable | | | |
| udpEntry | | | |
| | | udpEntryLocalAddress | RO |
| | | udpLocalPort | RO |

**egp:**

| | |
|---|---|
| egpInMsgs | RO |
| egpInErrs | RO |
| egpOutMsgs | RO |
| egpOutErrors | RO |
| egpNeighState | RO |
| egpNeighAddr | RO |
| egpNeighAs | RO |
| egpNeighInMsgs | RO |
| egpNeighInErrs | RO |
| egpNeighOutMsgs | RO |
| egpNeighOutErrs | RO |
| egpNeighInErrMsgs | RO |
| egpNeighOutErrMsgs | RO |
| egpNeighStateUps | RO |
| egpNeighStateDowns | RO |
| egpNeighIntervalHello | RO |
| egpNeighIntervalPoll | RO |
| egpNeighMode | RO |

**dsx1:**

dsx1ConfigTable

dsx1ConfigEntry

| | |
|---|---|
| dsx1LineIndex | RO |
| dsx1IfIndex | RO |
| dsx1TimeElapsed | RO |
| dsx1ValidIntervals | RO |
| dsx1LineType | RO |
| dsx1LineCoding | RO |
| dsx1SendCode | RO |

| | |
|---|---|
| dsx1CircuitIdentifier | RO |
| dsx1LoopbackConfig | RO |
| dsx1LineStatus | RO |
| dsx1SignalMode | RO |
| dsx1TransmitClockSource | RO |
| dsx1Fdl | RO |
| dsx1CurrentTable | |
| dsx1CurrentEntry | |
| dsx1CurrentIndex | RO |
| dsx1CurrentESs | RO |
| dsx1CurrentSESs | RO |
| dsx1CurrentSEFs | RO |
| dsx1CurrentUASs | RO |
| dsx1CurrentCSSs | RO |
| dsx1CurrentPCVs | RO |
| dsx1CurrentLESs | RO |
| dsx1CurrentBESs | RO |
| dsx1CurrentLCVs | RO |
| dsx1IntervalTable | |
| dsx1IntervalEntry | |
| dsx1IntervalIndex | RO |
| dsx1IntervalNumber | RO |
| dsx1IntervalESs | RO |
| dsx1IntervalSESs | RO |
| dsx1IntervalSEFs | RO |
| dsx1IntervalUASs | RO |
| dsx1IntervalCSSs | RO |
| dsx1IntervalPCVs | RO |

| | | | |
|---|---|---|---|
| | | dsx1IntervalLESs | RO |
| | | dsx1IntervalBESs | RO |
| | | dsx1IntervalLCVs | RO |
| dsx1TotalTable | | | |
| | dsx1TotalEntry | | |
| | | dsx1TotalIndex | RO |
| | | dsx1TotalESs | RO |
| | | dsx1TotalSESs | RO |
| | | dsx1TotalSEFs | RO |
| | | dsx1TotalUASs | RO |
| | | dsx1TotalCSSs | RO |
| | | dsx1TotalPCVs | RO |
| | | dsx1TotalLESs | RO |
| | | dsx1TotalBESs | RO |
| | | dsx1TotalLCVs | RO |
| dsx1FracTable | | | |
| | dsx1FracEntry | | |
| | | dsx1FracIndex | RO |
| | | dsx1FracNumber | RO |
| | | dsx1FractIfIndex | RO |

**snmp:**

| | |
|---|---|
| snmpInPkts | RO |
| snmpOutPkts | RO |
| snmpInBadVersions | RO |
| snmpInBadCommunityNames | RO |
| snmpInBadCommunityUses | RO |
| snmpInASNParseErrs | RO |
| snmpInTooBigs | RO |
| snmpInNoSuchNames | RO |
| snmpInBadValues | RO |
| snmpInReadOnlys | RO |
| snmpInGenErrs | RO |
| snmpInTotalReqVars | RO |
| snmpInTotalSetVars | RO |
| snmpInGetRequests | RO |
| snmpInSetRequests | RO |
| snmpInGetRequests | RO |
| snmpInTraps | RO |
| snmpOutTooBigs | RO |
| snmpOutNoSuchNames | RO |
| snmpOutBadValues | RO |
| snmpOutGenErrs | RO |
| snmpOutGetRequests | RO |
| snmpOutGetNexts | RO |
| snmpOutSetRequests | RO |
| snmpOutGetRepsonses | RO |
| snmpOutTraps | RO |
| snmpEnableAuthenTraps | RO |

**atm:**

atmInterfaceTable

atmInterfaceEntry

| | |
|---|---|
| atmInterfaceMaxVpcs | RO |
| atmInterfaceMaxVccs | RO |
| atmInterfaceConfVpcs | RO |
| atmInterfaceConfVccs | RO |
| atmInterfaceMaxActiveVpiBits | RO |
| atmInterfaceMaxActiveVciBits | RO |
| atmInterfaceIlmiVpi | RO |
| atmInterfaceIlmiVci | RO |
| atmInterfaceAddressType | RO |
| atmInterfaceAdminAddress | RO |
| atmInterfaceMyNeighborIpAddress | RO |
| atmInterfaceMyNeigherIfName | RO |

atmInterfaceTCTable

atmInterfaceTCEntry

| | |
|---|---|
| atmInterfaceOCDEvents | RO |
| atmInterfaceTCAlarmState | RO |

atmTrafficDescrParamTable

atmTrafficDescrParamEntry

| | |
|---|---|
| atmTrafficDescrParamIndex | RO |
| atmTrafficDescrType | RO |
| atmTrafficDescrParam1 | RO |
| atmTrafficDescrParam2 | RO |
| atmTrafficDescrParam3 | RO |
| atmTrafficDescrParam4 | RO |
| atmTrafficDescrParam5 | RO |

| | | | |
|---|---|---|---|
| | | atmTrafficDescrQosClass | RO |
| | | atmTrafficDescrRowStatus | RO |
| atmVclTable | | | |
| | atmVclEntry | | |
| | | atmVclVpi | RO |
| | | atmVclVci | RO |
| | | atmVclAdminStatus | RO |
| | | atmVclOperStatus | RO |
| | | atmVclLastChange | RO |
| | | atmVclReceiveTrafficDescrIndex | RO |
| | | atmVclTransmitTrafficDescrIndex | RO |
| | | atmVccAalType | RO |
| | | atmVccAal5CpcsTransmitSduSize | RO |
| | | atmVccAal5CpcsReceiveSduSize | RO |
| | | atmVccAal5EncapsType | RO |
| | | atmVclCrossConnectIdentifier | RO |
| | | atmVclRowStatus | RO |
| aal5VccTable | | | |
| | aal5VccEntry | | |
| | | aal5VccVpi | RO |
| | | aal5VccVci | RO |
| | | aal5VccCrcErrors | RO |
| | | aal5VccSarTimeOuts | RO |
| | | aal5VccOverSizedSDUs | RO |